ISSN 2222-8772

Математические Структуры и Моделирование

Выпуск 26
2012

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. Ф. М. ДОСТОЕВСКОГО
ФАКУЛЬТЕТ КОМПЬЮТЕРНЫХ НАУК

МАТЕМАТИЧЕСКИЕ СТРУКТУРЫ И МОДЕЛИРОВАНИЕ

Выпуск 26

Омск 2012

Математические структуры и моделирование. — Омск : Омский государственный университет, 2012. – Вып. 26. – 142 с.

ISSN 2222-8772 (print)
ISSN 2222-8799 (online)

Редакционная коллегия

А. А. Берс	доктор техн. наук, профессор, Институт систем информатики СО РАН им. А. П. Ершова. Новосибирск
Н. Ф. Богаченко	канд. физ.-мат. наук, доцент, Омский государственный университет им. Ф. М. Достоевского
В. Я. Волков	доктор техн. наук, профессор, зав. кафедрой начертательной геометрии, инженерной и машинной графики, Сибирская государственная автомобильно-дорожная академия (СибАДИ)
А. Г. Гринь	доктор физ.-мат. наук, профессор, кафедра кибернетики, Омский государственный университет им. Ф. М. Достоевского
С. И. Горлов	доктор физ.-мат. наук, профессор, Нижневартовский государственный гуманитарный университет
А. К. Гуц	доктор физ.-мат. наук, профессор, зав. кафедрой кибернетики, Омский государственный университет им. Ф. М. Достоевского
А. Н. Кабанов	канд. физ.-мат. наук, кафедра кибернетики, Омский государственный университет им. Ф. М. Достоевского
П. А. Корчагин	доктор техн. наук, профессор, Сибирская государственная автомобильно-дорожная академия (СибАДИ)
Д. Н. Лавров	главный редактор, канд. техн. наук, доцент, зав. каф. компьютерных технологий и сетей, Омский государственный университет им. Ф. М. Достоевского
A. A. Fedorenko	Ph.D., Researcher (CR1) at the French National Centre of Scientific Research (CNRS) Laboratoire de Physique de l'ENS-Lyon, France
V. Kreinovich	Ph.D., Professor, Computer Science Department, University of Texas at El Paso, Texas, USA

Адрес научной редакции

Россия, 644053, Омск-53, ул. Грозненская, 11
Омский государственный университет им. Ф. М. Достоевского
факультет компьютерных наук

E-mail: lavrov@omsu.ru

© ФГБОУ ВПО «Омский государственный университет им. Ф. М. Достоевского», 2012

МАТЕМАТИЧЕСКИЕ СТРУКТУРЫ и МОДЕЛИРОВАНИЕ

В журнале публикуются статьи, в которых излагаются результаты исследований по фундаментальной и прикладной математике, теоретической физике и размышления, касающиеся окружающей нас природы и общества.

Публикуются также статьи по информационным технологиям, компьютерным наукам, защите информации, философии и истории математики.

Объекты исследования должны быть представлены в форме некоторых математических структур и моделей.

Журнал является реферируемым. Рефераты статей публикуются в «Реферативном журнале» и в журналах «Zentralblat für Mathematik» (Германия) и «Mathematical Reviews» (США).

Электронная версия журнала представлена в сети Интернет по адресу:

http://msm.univer.omsk.su

Журнал издаётся на коммерческие средства факультета компьютерных наук Омского государственного университета.

Электронная почта редактора:

lavrov@omsu.ru

Подробную информацию можно найти на Web-сервере:

http://msm.univer.omsk.su

СОДЕРЖАНИЕ

Фундаментальная математика и физика

А.Г. Гринь. *О точности нормальной аппроксимации распределений сумм зависимых случайных величин* ... 5

С.С. Кутателадзе. *Дело Лузина — трагедия математики России* ... 20

В.Н. Степанов. *Уравнение первого рода относительно меры на сфере* S^{n-1} ... 38

L. Longpré, O. Kosheleva. *Towards Unique Physically Meaningful Definitions of Random and Typical Objects* ... 49

V. Kreinovich, A. Ortiz. *If Energy Is Not Preserved, Then Planck's Constant Is No Longer a Constant: A Theorem* ... 57

Прикладная математика и моделирование

А.К. Гуц. *Модель смены сознания сна и сознания реальности* ... 64

Компьютерные науки

А.В. Багма. *Обзор высокопроизводительных вычислительных платформ для графических ускорителей* ... 73

Д.Э. Вильховский, С.С. Ефимов. *Исследование алгоритмов определения изоморфности графов в системах с распределённой и общей памятью* ... 89

А.В. Макаренко, А.В. Пыхтеев, С.С. Ефимов. *Параллельная реализация и сравнительный анализ алгоритмов факторизации в системах с распределённой памятью* ... 94

К.В. Пугин, С.С. Ефимов. *Генетические алгоритмы с частичной параллелизацией в системах с общей памятью на примере задачи коммивояжёра* ... 110

Продолжение на следующей странице

С.В. Стопкин, К.В. Пугин, С.С. Ефимов. *Распознавание дорожной разметки на базе Intel OpenCV* 118

Информационная безопасность

А.Б. Лысак. *Идентификация и аутентификация личности: обзор основных биометрических методов проверки подлинности пользователя компьютерных систем* 124

Математические структуры и моделирование
2012, вып. 26, с. 5–19

УДК 519.214.5

О ТОЧНОСТИ НОРМАЛЬНОЙ АППРОКСИМАЦИИ РАСПРЕДЕЛЕНИЙ СУММ ЗАВИСИМЫХ СЛУЧАЙНЫХ ВЕЛИЧИН

А.Г. Гринь

Получены оценки скорости сходимости в предельных теоремах о сходимости к нормальному закону для последовательностей слабо зависимых случайных величин без предположения о существовании дисперсии.

1. Введение. Формулировки основных результатов

Пусть $\{\xi_n\} = \{\xi_n,\ n = 1, 2, ...\}$ — стационарная в узком смысле последовательность и пусть $\mathcal{F}_{\leqslant n}$ и $\mathcal{F}_{\geqslant n}$ — σ-алгебры, порождённые семействами $\{\xi_i : i \leqslant n\}$ и $\{\xi_i : i \geqslant n\}$. Говорят, что последовательность $\{\xi_n\}$ удовлетворяет *условию равномерно сильного перемешивания (φ-перемешивания)* с коэффициентом перемешивания $\varphi(n)$, если

$$\varphi(n) = \sup\left\{\frac{|\mathbf{P}(AB) - \mathbf{P}(A)\mathbf{P}(B)|}{\mathbf{P}(A)} :\ A \in \mathcal{F}_{\leqslant 0},\ B \in \mathcal{F}_{\geqslant n}\right\} \to 0,\quad n \to \infty.$$

Обозначим

$$T_n = \sum_{k=1}^{n} \xi_n,\ \xi_n(z) = \xi_n \mathbf{1}\left\{|\xi_n| \leqslant z\right\},\quad T_n(z) = \sum_{j=1}^{n} \xi_j(z),\quad \sigma_n(z) = \mathbf{D}T_n(z).$$

Введём так называемую универсальную нормирующую последовательность $\{b_n\}$:

$$b_n = \sup\{z \geqslant 0 : \sigma_n(z) \geqslant z\}$$

(см., например, [1]). Будем писать $\xi \stackrel{d}{=} \eta$, $\xi_n \stackrel{d}{\to} \eta$ в случаях, когда, соответственно, распределения ξ и η совпадают и $\{\xi_n\}$ сходится к η по распределению. Обозначим через $\mathcal{N}(0, 1)$ случайную величину, имеющую стандартное нормальное распределение. Для того, чтобы при некотором выборе нормирующих постоянных A_n и $B_n \to +\infty$ имело место соотношение

$$B_n^{-1}T_n - A_n \stackrel{d}{\to} \mathcal{N}(0, 1), \tag{1}$$

Copyright © 2012 **А.Г. Гринь**
Омский государственный университет им. Ф.М. Достоевского
E-mail: griniran@gmail.com

достаточно, а если $\varphi(1) < 1$ — и необходимо, чтобы при любом $\varepsilon > 0$

$$n\mathbf{P}\left\{|\xi_1| \geqslant \varepsilon b_n\right\} \to 0, \quad n \to \infty \tag{2}$$

При этом если выполнено (1) и $\varphi(1) < 1$, то $A_n = b_n^{-1} n\mathbf{E}\xi_1(b_n) + o(1)$, $B_n \sim b_n \sim \sigma_n(b_n)$, $\{b_n\}$ является правильно меняющейся последовательностью порядка $1/2$, и если $h(x)$ — медленно меняющаяся функция такая, что $nh(b_n) \sim b_n^2,\ n \to \infty$, то

$$P\left\{|\xi_1| \geqslant x\right\} \leqslant C\frac{h(x)}{x^2},\ C > 0 \tag{3}$$

[1, 2]. Обозначим

$$\Delta_n = \sup_x \left| \mathbf{P}\left\{\frac{T_n - n\mathbf{E}\xi_1(b_n)}{b_n} < x\right\} - \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} \exp\left\{-\frac{t^2}{2}\right\} dt \right|.$$

В дальнейшем будем писать $g \ll h$, если $g(t, n, ...) \leqslant ch(t, n, ...)$, где $c > 0$ не зависит от $t, n, ...$, а $g \asymp h$ будет обозначать, что $g \ll h$ и $h \ll g$. Основным результатом настоящей работы является следующая

Теорема 1. *Если $\{\xi_n\}$ удовлетворяет условию экспоненциально быстрого φ-перемешивания (то есть $\varphi(n) \leqslant e^{-\alpha n},\ \alpha > 0$), $\varphi(1) < 1$ и выполнено условие (2), то при любом $\varepsilon > 0$*

$$\Delta_n \ll n\mathbf{P}\left\{|\xi_1| \geqslant b_n\right\} + b_n^{-3} n\mathbf{E}|\xi_1(b_n)|^3 + n^{-\frac{1}{2}+\varepsilon}.$$

Теорему 1 можно интерпретировать как распространение неулучшаемых в определённом смысле верхних оценок П. Холла из [3] на последовательности слабо зависимых величин.

Следствие 1. Если $\{\xi_n\}$ удовлетворяет условию экспоненциально быстрого φ-перемешивания, $\varphi(1) < 1$, и $\mathbf{E}|\xi_1|^a < \infty,\ 2 < a < 3$, то $\Delta_n \ll n^{\frac{a}{2}-1}$.

Этот результат улучшает оценки А.Н. Тихомирова из [4].

Следствие 2. Если $\{\xi_n\}$ удовлетворяет условию экспоненциально быстрого φ-перемешивания и $P\left\{|\xi_1| \geqslant x\right\} = x^{-a}h(x),\ 2 \leqslant a < 3$, где $h(x)$ — медленно меняющаяся функция, то $\Delta_n \ll n\mathbf{P}\left\{|\xi_1| \geqslant b_n\right\}$.

Ясно, что при $a = 2$ у величин ξ_1 с указанным распределением дисперсия может и не существовать.

2. Вспомогательные результаты

Обозначим через $\mathcal{F}_{\leqslant n}$ и $\mathcal{F}_{\geqslant n}$ σ–алгебры, порождённые, соответственно, семействами $\{\xi_k : k \leqslant n\}$ и $\{\xi_k : k \geqslant n\}$.

Лемма 1. *Пусть последовательность $\{\xi_n\}$ удовлетворяет условию равномерно сильного перемешивания (φ–перемешивания) с коэффициентом перемешивания $\varphi(n)$ и пусть случайные величины ξ и η измеримы относительно $\mathcal{F}_{\leqslant 0}$ и $\mathcal{F}_{\geqslant n}$ соответственно,*

$$\|\xi\|_p = (\mathbf{E}|\xi|^p)^{\frac{1}{p}} < \infty, \quad \|\eta\|_q < \infty, \quad p > 1,\ q > 1, \quad p^{-1} + q^{-1} = 1.$$

Тогда при любых комплексных a и b

$$|\mathbf{E}\xi\eta - \mathbf{E}\xi\mathbf{E}\eta| \leqslant 2\varphi^{\frac{1}{p}}(n)\|\xi - a\|_p\|\eta - b\|_q. \tag{4}$$

Если же

$$\|\xi\|_1 = \mathbf{E}|\xi| < \infty,\ \|\eta\|_\infty = \operatorname{vrai\,sup}|\eta| \leqslant \infty,$$

то

$$|\mathbf{E}\xi\eta - \mathbf{E}\xi\mathbf{E}\eta| \leqslant 2\varphi(n)\|\xi - a\|_1\|\eta - b\|_\infty. \tag{5}$$

Доказательство леммы легко получается, например, из теоремы 17.2.3 в [5] или из [6, с.236].

В дальнейшем будем обозначать через $\theta_i = \theta_i(t, n, ...),\ i = 1, 2, \ldots$ — ограниченные величины, (т.е. $\sup\limits_{t,n,...} |\theta_i(t, n, ...)| < \infty$); обозначим также $\tilde{\xi} = \xi - \mathbf{E}\xi$.

Лемма 2. *1. Пусть $\sum\limits_{k=1}^{\infty} k\varphi^{\frac{1}{2}}(k) < \infty$. Тогда*

$$\sigma^2(z) = \mathbf{E}\tilde{\xi}_1^2(z) + 2\sum_{k=1}^{\infty} \mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{k+1}(z) < \infty \quad \textit{и} \quad \sup_n |\sigma_n^2(z) - n\sigma^2(z)| \ll \sigma_1^2(z).$$

2. Если $\sum\limits_{k=1}^{\infty} k\varphi^{\frac{1}{2}}(k) < \infty$, $\varphi(1) < 1$, выполнено соотношение (2) и $\ln p \asymp \ln n$, $\ln c_n \asymp \ln n$, то $\sigma_p^2(c_n) \sim p\sigma^2(c_n)$.

3. Если

$$\sum_{k=1}^{\infty} \varphi^{\frac{1}{3}}(k) < \infty, \quad \textit{то} \quad |\mathbf{E}\widetilde{T}_n^3(z)| \ll n\mathbf{E}|\tilde{\xi}_1(z)|^3.$$

4. В условиях пункта 2

$$\mathbf{E}\widetilde{T}_p^4(c_n) \ll p\mathbf{E}|\tilde{\xi}_1(c_n)|^4 + p^2\sigma^4(c_n).$$

5. Если

$$\sum_{k=1}^{\infty} \varphi(k) < \infty, \quad \textit{то} \quad \left|b_n^{-2}\sigma_n^2(b_n) - 1\right| \ll n\mathbf{P}\left\{|\xi_1| \geqslant b_n\right\}.$$

Доказательство. Имеем

$$\sigma_n^2(z) = n\mathbf{E}\tilde{\xi}_1^2(z) + 2\sum_{k=1}^{n-1}(n-k)\mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{k+1}(z).$$

С помощью леммы 1 получаем отсюда

$$|\,\sigma_n^2(z) - n\sigma^2(z)| = \left| 2n\sum_{k=n}^{\infty}\mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{k+1}(z) + 2\sum_{k=1}^{n-1}k\mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{k+1}(z)\right| \leqslant$$

$$\leqslant 4\sigma_1^2(z)\left(n\sum_{k=n}^{\infty}\varphi^{\frac{1}{2}}(k) + \sum_{k=1}^{n-1}k\varphi^{\frac{1}{2}}(k)\right) \leqslant 4\sigma_1^2(z)\sum_{k=1}^{\infty}k\varphi^{\frac{1}{2}}(k),$$

что доказывает утверждение 1 леммы.

Докажем утверждение 2. В наших предположениях справедливо соотношение (3), из которого следует, что $\sigma_1^2(b_n)$ и $\sigma_1^2(c_n)$ не превосходят некоторую медленно меняющуюся последовательность (см., например [5, с. 98]), так что $\sigma_1^2(b_n) = o(n^{\varepsilon})$ и $\sigma_1^2(b_n) = o(n^{\varepsilon})$ при любом $\varepsilon > 0$ [7, с. 24].

$\{b_n^2\}$ является правильно меняющейся последовательностью порядка 1, а в силу утверждения 1 $b_n^2 \sim \sigma_n^2(b_n) = n\sigma^2(b_n) + \theta_1\sigma_1(b_n)$, следовательно $b_n^2 \sim n\sigma^2(b_n)$ и $\sigma^2(b_n)$, а вместе с ней и $\sigma^2(n)$ являются медленно меняющимися последовательностями. Из утверждения 1 настоящей леммы выводим теперь

$$\sigma_p^2(c_n) = p\sigma^2(c_n) + \theta_2\sigma_1^2(c_n) \sim p\sigma^2(c_n).$$

Доказательство утверждения 3.

В силу стационарности последовательности $\{\xi_n(z)\}$

$$\left|\mathbf{E}\widetilde{T}_n^3(z)\right| \leqslant 6n\sum_{0\leqslant i+j\leqslant n-1}\left|\mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{i+1}(z)\tilde{\xi}_{i+j+1}(z)\right|. \tag{6}$$

С помощью соотношения (4) (справедливого и при $n = 0,\ \varphi(0) = 1$) получаем

$$\left|\mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{i+1}(z)\tilde{\xi}_{i+j+1}(z)\right| \leqslant 2\varphi^{\frac{2}{3}}(i)\|\tilde{\xi}_1(z)\|_3\|\tilde{\xi}_{i+1}(z)\tilde{\xi}_{i+j+1}(z)\|_{\frac{3}{2}} \leqslant 2\varphi^{\frac{2}{3}}(i)\|\tilde{\xi}_1(z)\|_3^3,$$

$$\left|\mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{i+1}(z)\tilde{\xi}_{i+j+1}(z)\right| \leqslant 2\varphi^{\frac{2}{3}}(j)\|\tilde{\xi}_{i+j+1}(z)\|_3\|\tilde{\xi}_1(z)\tilde{\xi}_{i+1}(z)\|_{\frac{3}{2}} \leqslant 2\varphi^{\frac{2}{3}}(j)\|\tilde{\xi}_1(z)\|_3^3.$$

Отсюда

$$\left|\mathbf{E}\tilde{\xi}_1(z)\tilde{\xi}_{i+1}(z)\tilde{\xi}_{i+j+1}(z)\right| \leqslant 2(\varphi(i)\varphi(j))^{\frac{1}{3}}\|\tilde{\xi}_1(z)\|_3^3. \tag{7}$$

Из (6) и (7) следует утверждение 2.

Доказательство утверждения 4. Воспользуемся известным неравенством М. Пелиград [8]:

пусть при некоторых $a > 0,\ \delta > 0$ и натуральном m

$$\varphi(m) + \max_{1\leqslant j\leqslant p}\mathbf{P}\{|\widetilde{T}_j(c_n)| \geqslant \delta a\} \leqslant \gamma < 1.$$

Тогда при любых $x \geqslant a$ и $p \geqslant m$

$$\mathbf{P}\{|\widetilde{T}_p(c_n)| \geqslant x\} \leqslant \frac{\gamma}{1-\gamma}\mathbf{P}\left\{|\widetilde{T}_p(c_n)| \geqslant \frac{x}{1+4\delta}\right\} + \frac{p}{1-\gamma}\mathbf{P}\left\{|\tilde{\xi}_1(c_n)| \geqslant \frac{\delta x}{m(1+4\delta)}\right\}.$$

При $p/2 \leqslant j \leqslant p$ из неравенства Чебышёва и утверждения 1 следует

$$\mathbf{P}\{|\widetilde{T}_j(c_n)| \geqslant N\sqrt{p}\sigma(c_n)\} \leqslant \frac{\sigma_j^2(c_n)}{N^2 p\sigma^2(c_n)} \leqslant \frac{1}{N^2}.$$

Если же $j < p/2$, то с помощью полученного неравенства выводим

$$\mathbf{P}\{|\widetilde{T}_j(c_n)| \geqslant N\sqrt{p}\sigma(c_n)\} \leqslant \mathbf{P}\{|\widetilde{T}_p(c_n)| \geqslant N\sqrt{p}\sigma(c_n)/2\} +$$

$$+\mathbf{P}\{|\widetilde{T}_p(c_n) - \widetilde{T}_j(c_n)| \geqslant N\sqrt{p}\sigma(c_n)/2\} \leqslant \frac{8}{N^2}.$$

Два последних неравенства означают, что неравенство М. Пелиград справедливо при $a = N\sqrt{p}\sigma(c_n)$, причём $N > 0$ и $m \in \mathbb{N}$ можно выбрать такими, чтобы $\dfrac{\gamma(1+4\delta)^4}{1-\gamma} < 1$. Имеем

$$\mathbf{E}\widetilde{T}_p^4(c_n) = \int_0^\infty \mathbf{P}\{\widetilde{T}_j^4(c_n) \geqslant x\}\,dx \leqslant N^4p^2\sigma^4(c_n) +$$

$$+\frac{\gamma}{1-\gamma}\int_{N\sqrt{p}\sigma(c_n)}^\infty \mathbf{P}\left\{\widetilde{T}_p^4(c_n) \geqslant \frac{x}{(1+4\delta)^4}\right\}dx +$$

$$+\frac{p}{1-\gamma}\int_{N\sqrt{p}\sigma(c_n)}^\infty \mathbf{P}\left\{\tilde{\xi}_1^4(c_n) \geqslant \frac{\delta^4 x}{m^4(1+4\delta)^4}\right\}dx \leqslant$$

$$\leqslant \frac{\gamma(1+4\delta)^4}{1-\gamma}\mathbf{E}\widetilde{T}_p^4(c_n) + p\frac{m^4(1+4\delta)^4}{(1-\gamma)\delta^4}\mathbf{E}\tilde{\xi}_1^4(c_n),$$

отсюда следует утверждение 3.

Докажем утверждение 4. Обозначим $\delta_n = n\mathbf{P}\{|\xi_1| > b_n\}$. В силу определения b_n существует последовательность положительных чисел $d_n \geqslant b_n$ такая, что $0 \leqslant d_n^{-2}\sigma_n^2(d_n) - 1 \leqslant \delta_n$ и $0 < d_n^2 b_n^{-2} - 1 \leqslant \delta_n$. Тогда

$$|b_n^{-2}\sigma_n^2(d_n) - 1| \ll \delta_n. \tag{8}$$

Далее, обозначим

$$W_n = \widetilde{T}_n(d_n) - \widetilde{T}_n(b_n) = \sum_{j=1}^n \eta_j, \quad \eta_j = \tilde{\xi}_j \mathbf{1}\{b_n < |\xi_j| \leqslant d_n\}, \ \ j = 1, ..., n.$$

Тогда

$$\sigma_n^2(d_n) = \sigma_n^2(b_n) + 2\mathbf{E}\widetilde{T}_n(b_n)W_n + \mathbf{E}W_n^2. \tag{9}$$

В силу соотношения (5)

$$\left|\mathbf{E}\tilde{\xi}_i(b_n)\eta_j\right| \leqslant 2\varphi(|i-j|)\|\xi_i(b_n)\|_\infty\|\xi_j\mathbf{1}\left\{b_n < |\xi_j| \leqslant d_n\right\}\|_1 \ll \varphi(|i-j|)b_n d_n\mathbf{P}\left\{|\xi_j| > b_n\right\},$$

откуда

$$\mathbf{E}\widetilde{T}_n(b_n)W_n \ll nb_n d_n\mathbf{P}\left\{|\xi_j| > b_n\right\}. \tag{10}$$

Аналогично показывается, что

$$\mathbf{E}W_n^2 \ll nd_n^2\mathbf{P}\left\{|\xi_j| > b_n\right\}. \tag{11}$$

Так как $d_n^2 \ll b_n^2$, то из (8), (9), (10) и (11) следует утверждение 4.

3. Доказательство основных результатов

Пусть n и p — натуральные числа, $\{c_n\}$ и $\{d_n\}$ — последовательности положительных чисел. Ниже с помощью конструкции из [9] выводится представление для характеристических функций величин $\widetilde{T}_n(c_n)$.

Обозначим

$$Q_j(c_n) = d_n^{-1}\sum_{l=1}^{p}\tilde{\xi}_{(j-1)p+l}(c_n), \quad f_r(t) = \mathbf{E}\exp\left\{it\sum_{j=1}^{r}Q_j(c_n)\right\}, \quad j,r = 1,2,...$$

Введём функцию

$$F_k(z) = \mathbf{E}\prod_{j=1}^{k}\left(f_1 + z\left(\exp\left\{itQ_j(c_n)\right\} - f_1\right)\right) = \sum_{m=1}^{k}z^m f_1^{k-m}\mathbf{E}S_m(X_1,...,X_k),$$

где $X_j = \exp\left\{itQ_j(c_n)\right\} - f_1,\ j = 1,...,k$, а

$$S_0(x_1,...,x_k) = 1, \quad S_m(x_1,...,x_k) = \sum_{1\leqslant j_1<...<j_m\leqslant k}x_{j_1}...x_{j_k} -$$

— m-й элементарный симметрический многочлен. Из формулы Тейлора для функции $F_k(z)$ (см., например, [10, с. 67]) получаем при $l < k$

$$f_k(t) = F_k(1) = f_1^k + f_1^{k-1}\mathbf{E}S_1(X_1,...,X_k) + ... + f_1^{k-l}\mathbf{E}S_l(X_1,...,X_k) + R_l, \tag{12}$$

где

$$R_l = R_l(X_1,...,X_k) = \frac{1}{2\pi i}\int\limits_{|z|=\rho}\frac{F_k(z)\,dz}{(z-1)\,z^{l+1}}, \quad |\rho| > 1. \tag{13}$$

Обозначим $g_l = \mathbf{E}X_1...X_l,\ l \geqslant 1,\ \beta^2 = \mathbf{E}|X_1|^2 = 1 - |f_1|^2$.

Лемма 3. *Пусть выполняются условия Теоремы 1. Положим в определении* $f_r(t)$ $d_n = \sigma_n(c_n)$. *Тогда*

1. $$\mathbf{E}S_1(X_1,...,X_k) = 0,\ \mathbf{E}S_2(X_1,...,X_k) = (k-1)g_2 + O(\beta^2 k^2 \varphi^{\frac{1}{2}}(p)),$$

$$\mathbf{E}S_3(X_1,...,X_k) = (k-2)g_3 + O(\beta^2 k^3 \varphi^{\frac{1}{2}}(p)). \tag{14}$$

2. Пусть $n = kp$. *Существует* $\gamma > 0$ *такое, что при* $|t| \leqslant \gamma\sigma_n(c_n)\sigma_p^{-1}(c_n)$

$$f_1(t) = \exp\left\{-\frac{t^2\sigma_p^2(c_n)}{2\sigma_n^2(c_n)} + \theta_3\Psi(n,t,c_n)\right\}, \tag{15}$$

где

$$\Psi(n,t,c_n) = \frac{p\mathbf{E}|\tilde{\xi}_1(c_n)|^3}{\sigma_n^3(c_n)}|t|^3 + \frac{p\mathbf{E}\tilde{\xi}_1^4(c_n)}{\sigma_n^4(c_n)}t^4 + \frac{t^4}{k^2}.$$

3. Пусть $g_2^* = f_1^{-2}g_2,\ g_3^* = f_1^{-3}g_3$. *При* $|t| \leqslant \gamma\sigma_n(c_n)\sigma_{3p}^{-1}(c_n)$

$$|g_2^*| \ll \frac{\sigma_1^2(c_n)}{\sigma_n^2(c_n)}t^2 + \theta_4\Psi(n,t,c_n),\ |g_3^*| \ll \frac{\sigma_1^2(c_n)}{\sigma_n^2(c_n)}t^2 + \theta_5\Psi(n,t,c_n). \tag{16}$$

Доказательство. 1. Так как $\mathbf{E}X_j = 0,\ j = 1,2,...,$ то

$$\mathbf{E}S_1(X_1,...,X_k) = \mathbf{E}\sum_{j=1}^{k} X_j = 0.$$

В сумме $\mathbf{E}S_2(X_1,...,X_k)$ имеется $k-1$ слагаемое вида $\mathbf{E}X_jX_{j+1} = g_2$ и $(k-1)(k-2)/2$ слагаемых вида $\mathbf{E}X_jX_l,\ |j-l| > 1$, каждое из которых по лемме 1 не превосходит $2\varphi^{\frac{1}{2}}(p)\|X_j\|_2\|X_l\|_2 = 2\beta^2\varphi^{\frac{1}{2}}(p)$; это даёт нам нужную оценку для $\mathbf{E}S_2(X_1,...,X_k)$. Соотношение (14) доказывается аналогично.

2. При $|t| \leqslant \gamma\sigma_n(c_n)\sigma_p^{-1}(c_n)$. С помощью утверждения 2 леммы 2 получаем

$$|f_1(t) - 1| \leqslant \frac{t^2\sigma_p^2(c_n)}{2\sigma_n^2(c_n)} \leqslant \frac{\gamma}{2},\quad |f_1(t) - 1|^2 \leqslant \frac{t^4\sigma_p^4(c_n)}{4\sigma_n^4(c_n)} \ll \frac{t^4}{k^2}, \tag{17}$$

а из (17) выводим

$$\ln f_1(t) = f_1(t) - 1 + \theta_6|f_1(t) - 1|^2 =$$

$$= -\frac{t^2\sigma_p^2(c_n)}{2\sigma_n^2(c_n)} + \frac{\mathbf{E}\widetilde{T}_p^3(c_n)}{6\sigma_n^3(c_n)}(it)^3 + \theta_7\left(\frac{\mathbf{E}\widetilde{T}_p^4(c_n)}{\sigma_n^4(c_n)}t^4 + \frac{t^4}{k^2}\right).$$

Отсюда уже легко выводится (15).

3. Нетрудно подсчитать, что $g_2^* = \left(f_1^{-2}f_2 - 1\right)$. Представив f_1 и f_2 в виде (15) и воспользовавшись леммой 2, получим при $|t| \leqslant \gamma\sigma_n(c_n)\sigma_{2p}^{-1}(c_n)$

$$f_2f_1^{-2} = \exp\left\{-\frac{\sigma_{2p}^2(c_n) - 2\sigma_p^2(c_n)}{2\sigma_n^2(c_n)}t^2 + \theta_8\Psi(n,t,c_n)\right\} =$$

$$= \exp\left\{\theta_9 \frac{\sigma_1^2(c_n)}{\sigma_n^2(c_n)} t^2 + \theta_{10}\Psi(n,t,c_n)\right\} = e^w.$$

В силу (17) при достаточно малых $\gamma > 0$ $|e^w| = |f_2 f_1^{-2}| \leqslant 4$, и

$$\left|\frac{e^w - 1}{w}\right| \leqslant e,\ |w| \leqslant 1, \quad \left|\frac{e^w - 1}{w}\right| \leqslant |e^w - 1| \leqslant 5,\ |w| > 1,$$

так что из приведённого выше представления для e^w следует оценка для $|g_2^*|$ в (16). Далее $g_3^* = \left(f_1^{-3} f_3 - 1\right) - 2g_2^* - g_2^{**}$, $g_2^{**} = \mathbf{E} X_1 X_3$. Представив входящие в определение g_3^* характеристические функции в виде (15), аналогично оценке для $|g_2^*|$ выводим (16).

Пусть $2q < p$. Обозначим

$$U_j = \frac{1}{\sigma_n(c_n)} \sum_{l=1}^{p-2q} \tilde{\xi}_{(j-1)p+q+l}(c_n), \quad V_j = \frac{1}{\sigma_n(c_n)} \sum_{l=1}^{q} (\tilde{\xi}_{(j-1)p+l}(c_n) + \tilde{\xi}_{jp-q+l}(c_n)),$$

$$u = u(t) = \mathbf{E}\exp\{itU_1\}, \quad v = v(t) = \mathbf{E}\exp\{itV_1\}.$$

Тогда $Q_j(c_n) = U_j + V_j$, $X_j = Y_j + Z_j$, $j = 1, 2, ...,$ где

$$Y_j = (\exp\{itU_j\} - u)v, \quad Z_j = \exp\{itU_j\}(\exp\{itV_j\} - v) + uv - f_1,$$

так что

$$F_k(z) = \mathbf{E}\prod_{j=1}^{k} \left(f_1 + z\left(Y_j + Z_j\right)\right). \tag{18}$$

Лемма 4.

$$|F_k(z)| \leqslant \left\{1 - \beta^2 + \rho^2\delta^2 + 8\rho^2\varphi(p)\right\}^{\frac{k}{2}} + 16\rho\varphi(q)B_k, \tag{19}$$

где $\delta^2 = 1 - |v|^2$, $\rho = |z| \geqslant 1$, *а*

$$B_k = \sum_{l=2}^{k-2} \|\prod_{j=1}^{l-1}(f_1 + zX_j)\|_\infty \left\{1 - \beta^2 + \rho^2\delta^2 + 8\rho^2\varphi(p)\right\}^{\frac{k-l-1}{2}} +$$

$$+ \|\prod_{j=1}^{k-1}(f_1 + zX_j)\|_\infty \left\{1 - \beta^2 + \rho^2\delta^2 + 8\rho^2\varphi(p)\right\}^{\frac{k-2}{2}}.$$

Доказательство практически дословно повторяет рассуждения леммы 8 в [9].

Обозначим $\delta_n = n\mathbf{P}\left\{|\xi_1| \geqslant b_n\right\}$, $\tau_n = \dfrac{n\mathbf{E}|\tilde{\xi}_1(b_n)|^3}{b_n^3}$.

Лемма 5. *Пусть* $k = k(n) = [n^a]$, $a = 1 - \dfrac{1}{\sqrt{2}}$, $n = kp$, $k_1 = k(p)$, $\psi_n = \gamma\min(\sqrt{k_1}, \tau_n^{-\frac{1}{2}})$. *В условиях теоремы 1 существует* $\gamma > 0$ *такое, что при* $n^{-1} \leqslant |t| \leqslant \psi_n$

$$f_n^*(t) = \mathbf{E}\exp\left\{it\frac{\widetilde{T}_n(b_n)}{b_n}\right\} = \exp\left\{-\frac{t^2}{2} + \theta_{11}\left(\delta_n t^2 + \frac{t^2 + t^4}{n^{\frac{1}{2}-\varepsilon}} + \tau_n(|t|^3 + t^4)\right)\right\}. \tag{20}$$

Д о к а з а т е л ь с т в о.
Пусть $n^{-1} \leqslant |t| \leqslant \gamma\sigma_n(c_n)\sigma_p^{-1}(c_n) \sim \gamma\sqrt{k}$ (см. лемму 2). Положим

$$p = \left[\frac{n}{k}\right], \quad q = \left[p^{\frac{2}{3}}k^{-\frac{1}{3}}\right].$$

Тогда, кстати, $kq = o(p)$. При достаточно малых $\gamma > 0$

$$\beta^2 = \mathbf{E}\left|\exp\{itX_1\} - f_1\right|^2 \leqslant \mathbf{E}\left|\exp\{itX_1\} - 1\right|^2 \leqslant \frac{t^2\sigma_p^2(c_n)}{2\sigma_n^2(c_n)} < \frac{1}{2}. \tag{21}$$

Аналогично с помощью леммы 2 выводим

$$\delta^2 = 1 - |v(t)|^2 \leqslant \frac{t^2}{2}\mathbf{D}V_1 \sim \frac{t^2\sigma_q^2(c_n)}{\sigma_n^2(c_n)}. \tag{22}$$

Так как $|v(t)|^2$ является характеристической функцией случайной величины $W = V_1 - \widehat{V}_1$, где V_1 и $\widehat{V}_1$ независимы и одинаково распределены и $3(1-\cos x) \geqslant x^2$, $|x| \leqslant 1$, то

$$\delta^2 = 1 - \mathbf{E}\cos(tW) \geqslant \frac{t^2}{3}\mathbf{E}W^2\mathbf{1}\left\{|tW| \leqslant 1\right\}. \tag{23}$$

Далее, с помощью утверждения 2 леммы 2 выводим

$$\mathbf{D}W = 2\mathbf{D}V_1 \ll \sigma_n^{-2}(c_n)\sigma_q^2(c_n) \ll \sigma_n^{-2}(c_n)\sigma_p^2(c_n),$$

так что при $|t| \leqslant \gamma\sigma_n^{-2}(c_n)\sigma_p^{-1}(c_n)$

$$\{|tW| \leqslant 1\} \supseteq \{|W| \leqslant C\gamma^{-1}\sqrt{\mathbf{D}W}\},$$

где $C > 0$ не зависит от n и γ. Далее, из леммы 4 в [1] следует

$$\mathbf{E}W^2\mathbf{1}\left\{|W| \geqslant C\gamma^{-1}\sqrt{\mathbf{D}W}\right\} = o_\gamma(1)\mathbf{D}W,$$

и при достаточно малых $\gamma > 0$ и достаточно больших n из (23) следует теперь

$$\delta^2 \geqslant \frac{t^2}{4}\mathbf{D}W \geqslant t^2\sigma_n^{-2}(c_n)\sigma_q^2(c_n). \tag{24}$$

Из (12) и (13) при $l = 3$ с помощью утверждения 1 леммы 3 получаем

$$f_k(t) = f_1^k(t)\left(1 + (k-1)g_2^* + (k-2)g_3^* + \theta_{12}\beta^2k^3\varphi^{\frac{1}{2}}(p)\right) + R_3, \tag{25}$$

$$|R_3| = \left|\frac{1}{2\pi i}\int\limits_{|z|=\rho}\frac{F_k(z)\,dz}{(z-1)\,z^4}\right| \leqslant (\rho-1)^{-1}\rho^{-3}\sup_{|z|=\rho}|F_k(z)|, \quad |\rho| > 1. \tag{26}$$

Положим в (26) $\rho^2 = \dfrac{1-\beta^2}{k\delta^2}$. При достаточно малых γ и достаточно больших n с помощью (21), (22) и утверждения 2 леммы 2 получаем

$$\rho^{-2} \leqslant 2\frac{kt^2\sigma_q^2(c_n)}{\sigma_n^2(c_n)} \leqslant 2\gamma^2\frac{kq}{p} \leqslant \frac{1}{2} \quad \text{при} \quad |t| \leqslant \gamma\sigma_n^{-2}(c_n)\sigma_p^{-1}(c_n),$$

а при $|t| \geqslant n^{-1}$ с помощью (24) —

$$\rho^2 \leqslant \frac{b_n^2}{kt^2\sigma_q^2(c_n)} \ll n^2.$$

Используя два последних неравенства, лемму 2, лемму 4, соотношения (19) и (26), выводим

$$|R_3| \ll f_1^k \frac{k^{\frac{3}{2}}\sigma_q^3(c_n)|t|^3}{\sigma_n^3(c_n)} \left(1 + \frac{1}{k} + n^2\varphi(p)\right)^{\frac{k}{2}} + t^2n^3\varphi(q)B_k \ll$$

$$\ll f_1^k \frac{\mathbf{E}|\widetilde{T}_p(c_n)|^3|t|^3}{\sigma_n^3(c_n)} + t^2n^3\varphi(q)B_k, \tag{27}$$

где

$$B_k \leqslant k(1+2\rho)^k \left(1 + \frac{1}{k} + n^2\varphi(p)\right)^{\frac{k}{2}} \ll k(1+n^2)^k.$$

По условию $\varphi(n) \leqslant \exp\{-\alpha n\}$ и так как $k\ln n = o(q)$, то из последнего неравенства следует

$$n^3\varphi(q)B_k \ll \exp\left\{3\ln n + k\ln(1+n^2) - \alpha q\right\} \ll e^{-\alpha' q}, 0 < \alpha' < \alpha. \tag{28}$$

Из (16), (25) и (28) получаем

$$f_k(t) = f_1^k(t)\left[1 + \theta_{13}\left(\frac{\sigma_1^2(c_n)}{\sigma_n^2(c_n)}t^2 + k\Psi(n,t,c_n)\right)\right] + \theta_{14}t^2\exp\left\{-\alpha' q\right\}.$$

Так как $\sigma_1(n)$ и $\sigma(n)$ — медленно меняющиеся функции (см. доказательство утверждения 2 леммы 2), то $\sigma_1^2(c_n)\sigma_n^{-2}(c_n) = o(n^{1-2\varepsilon})$ при любом $\varepsilon > 0$, поэтому последнее соотношение можно переписать так

$$f_k(t) = f_1^k(t)\left[1 + \theta_{15}\left(\frac{t^2}{n^{1-2\varepsilon}} + k\Psi(n,t,c_n)\right)\right] + \theta_{16}t^2\exp\left\{-\alpha' q\right\}. \tag{29}$$

Далее, из (15) и леммы 2 следует

$$f_1^k(t) = \exp\left\{-\frac{kt^2\sigma_p^2(c_n)}{2\sigma_n^2(c_n)} + \theta_{17}k\Psi(n,t,c_n)\right\}. \tag{30}$$

Из леммы 2, аналогично тому, как при выводе (29), получаем $\dfrac{k\sigma_p^2(c_n)}{2\sigma_n^2(c_n)} = 1 + o(n^{-1+2\varepsilon})$, так что из (29) и (30) следует теперь

$$f_1^k(t) = \exp\left\{-\frac{t^2}{2} + \theta_{18}\left(\frac{t^2}{n^{1-2\varepsilon}} + k\Psi(n,t,c_n)\right)\right\}. \tag{31}$$

Обозначим

$$\mu_n^{-1} = \max\left\{\frac{n\mathbf{E}|\tilde{\xi}_1(c_n)|^3}{\sigma_n^3(c_n)}, \left(\frac{n\mathbf{E}\tilde{\xi}_1^4(c_n)}{\sigma_n^4(c_n)}\right)^{\frac{1}{2}}\right\}.$$

Нетрудно видеть, что если $|t| \leqslant \gamma \min(\sqrt{k}, \mu_n)$, то $k\Psi(n,t,c_n) \ll \gamma t^2$, откуда легко выводится, что при достаточно малых $\gamma > 0$

$$n \exp\{-\alpha' q\} = o\left(\exp\left\{-\frac{t^2}{2} + \theta_{19}\left(\frac{t^2}{n^{1-2\varepsilon}} + k\Psi(n,t,c_n)\right)\right\}\right),$$

что вместе с (29) и (31) даёт нам

$$f_k(t) = \mathbf{E}\exp\left\{it\frac{\widetilde{T}_n(c_n)}{\sigma_n(c_n)}\right\} = \exp\left\{-\frac{t^2}{2} + \theta_{20}\left(\frac{t^2}{n^{1-2\varepsilon}} + k\Psi(n,t,c_n)\right)\right\}. \qquad (32)$$

$|t| \leqslant \gamma \min(\sqrt{k}, \mu_n)$.

Обозначим $k_1 = k_1(n) = k(p) = [p^a]$ и пусть $k_1 p_1 = p$. Последовательность $\{c_n\}$ выберем так, чтобы $c_p = b_n$. Заменив в (32) n на p, k на k_1, и p на p_1, получим

$$\mathbf{E}\exp\left\{it\frac{\widetilde{T}_p(b_n)}{\sigma_p(b_n)}\right\} = \exp\left\{-\frac{t^2}{2} + \theta_{21}\left(\frac{t^2}{p^{1-2\varepsilon}} + k_1\Psi(p,t,b_n)\right)\right\}.$$

$|t| \leqslant \gamma \min(\sqrt{k_1}, \mu_p)$, откуда

$$f_1(t) = \mathbf{E}\exp\left\{it\frac{\widetilde{T}_p(b_n)}{\sigma_n(b_n)}\right\} =$$

$$= \exp\left\{-\frac{t^2\sigma_p^2(b_n)}{2\sigma_n^2(b_n)} + \theta_{22}\left(\frac{t^2\sigma_p^2(b_n)}{\sigma_n^2(b_n)p^{1-2\varepsilon}} + k_1\Psi\left(p, \frac{t\sigma_p(b_n)}{\sigma_n(b_n)}, b_n\right)\right)\right\}, \qquad (33)$$

$|t| \leqslant \gamma \min(\sqrt{k_1}, \mu_p)\sigma_n(b_n)\sigma_p^{-1}(b_n)$.

Далее, $\sigma_n(b_n) \sim b_n$, $kk_1 \sim n^{a+a(1-a)} = \sqrt{n}$, а $\sigma_p(b_n)\sigma_n^{-1}(b_n) \sim \sqrt{k}$ в силу леммы 2. Так как $b_n^{-4}\mathbf{E}|\tilde{\xi}_1(b_n)|^4 \leqslant b_n^{-3}\mathbf{E}|\tilde{\xi}_1(b_n)|^3$, то

$$\frac{1}{\sqrt{k}\mu_p} = \frac{1}{\sqrt{k}}\max\left\{\frac{p\mathbf{E}|\tilde{\xi}_1(b_n)|^3}{\sigma_p^3(b_n)}, \left(\frac{p\mathbf{E}\tilde{\xi}_1^4(b_n)}{\sigma_n^4(b_n)}\right)^{\frac{1}{2}}\right\} \leqslant \max(\tau_n, \sqrt{\tau_n}).$$

При $\tau_n > 1$ утверждение теоремы 1 выполняется очевидным образом, поэтому будем считать, что $\tau_n \leqslant 1$, в этом случае $\sqrt{k}\mu_p \geqslant \tau_n^{-\frac{1}{2}}$. Поскольку

$$k_1\Psi\left(p, \frac{t\sigma_p(b_n)}{\sigma_n(b_n)}, b_n\right) \sim \frac{p\mathbf{E}|\tilde{\xi}_1(b_n)|^3}{\sigma_n^3(b_n)}|t|^3 +$$

$$+\frac{p\mathbf{E}\tilde{\xi}_1^4(b_n)}{\sigma_n^4(b_n)}t^4 + \frac{t^4}{k\sqrt{n}} \leqslant \frac{p\mathbf{E}|\tilde{\xi}_1(b_n)|^3}{b_n^3}(|t|^3 + t^4) + \frac{t^4}{k\sqrt{n}},$$

то (33) можно переписать в виде

$$f_1(t) = \exp\left\{-\frac{t^2\sigma_p^2(b_n)}{2\sigma_n^2(b_n)} + \theta_{23}\Psi_1(t,n)\right\}, \text{ где} \qquad (34)$$

$$\Psi_1(t,n)=\frac{t^2}{kp^{1-2\varepsilon}}+\frac{p\mathbf{E}|\tilde{\xi}_1(b_n)|^3}{b_n^3}(|t|^3+t^4)+\frac{t^4}{k\sqrt{n}},$$

$|t|\leqslant\psi_n=\gamma\min\left(\sqrt{k_1},\tau_n^{-\frac{1}{2}}\right)$. Представив в виде (34) функцию f_2 и, проведя рассуждения, приводящие к утверждению 3 леммы 3, можно получить оценку

$$|g_2^*|\ll\frac{\sigma_1^2(b_n)}{\sigma_n^2(b_n)}t^2+\Psi_1(t,n),\quad |g_3^*|\ll\frac{\sigma_1^2(b_n)}{\sigma_n^2(b_n)}t^2+\Psi_1(t,n). \tag{35}$$

Если теперь повторить рассуждения, приводящие к (32), используя (34) и (35) вместо (15) и (16), получим

$$\mathbf{E}\exp\left\{it\frac{\widetilde{T}_n(b_n)}{\sigma_n^{-1}(b_n)}\right\}=\exp\left\{-\frac{t^2}{2}+\theta_{24}\left(\frac{t^2}{p_1^{1-2\varepsilon}}+\tau_n(|t|^3+t^4)+\frac{t^4}{\sqrt{n}}\right)\right\}, \tag{36}$$

$|t|\leqslant\psi_n$. В силу утверждения 5 леммы 2

$$\left|\frac{\sigma_n^2(b_n)}{b_n^2}-1\right|\ll\delta_n=n\mathbf{P}\left\{|\xi_1|\geqslant b_n\right\},$$

а $p_1=p(p)=\left(n^{\frac{1}{\sqrt{2}}}\right)^{\frac{1}{\sqrt{2}}}=\sqrt{n}$, так что из (36) следует теперь

$$f_n^*(t)=\mathbf{E}\exp\left\{it\frac{\widetilde{T}_n(b_n)}{b_n}\right\}=\exp\left\{-\frac{t^2}{2}+\theta_{25}\Psi_2(t,n)\right\}, \tag{37}$$

$$\Psi_2(t,n)=\delta_n t^2+\frac{t^2+t^4}{n^{\frac{1}{2}-\varepsilon}}+\tau_n(|t|^3+t^4),\ |t|\leqslant\psi_n.$$

Лемма доказана.

Лемма 6. *В условиях леммы 5*

$$\left|f_n^*(t)-\exp\left\{-\frac{t^2}{2}\right\}\right|\ll\Psi_2(t,n)\exp\left\{-\frac{t^2}{3}\right\},\ |t|\leqslant\psi_n.$$

Доказательство. Легко видеть, что при достаточно малых $\gamma>0$ если $|t|\leqslant\psi_n=\gamma\min\left(\sqrt{k_1},\tau_n^{-\frac{1}{2}}\right)$, то $|\theta_{25}|\Psi_2(t,n)\leqslant\dfrac{t^2}{6}$ (напомним, что мы рассматриваем только случай, когда $|\tau_n|\leqslant 1$, в противном случае утверждение теоремы 1 очевидно). С помощью неравенства $|\exp\{z\}-1|\leqslant|z|\exp\{|z|\}$ из (37) выводим теперь

$$\left|f_n^*(t)-\exp\left\{-\frac{t^2}{2}\right\}\right|\leqslant\exp\left\{-\frac{t^2}{2}\right\}|\theta_{25}|\Psi_2(t,n)\exp\left\{\frac{t^2}{6}\right\},$$

откуда следует утверждение леммы.

Лемма 7. *В условиях теоремы 1 при* $|t| \ll n^{\frac{1}{2}-\varepsilon}$

$$|f_n^*(t)| \ll \exp\left\{-\frac{t^2}{4}\right\} + o\left(e^{-n^\varepsilon}\right), \quad n \to \infty.$$

Доказательство.

Положим в (19) $z = \rho = 1,\ q = [Nn^\varepsilon], p = [N^2 n^\varepsilon],\ k = [np^{-1}],\ N > 0,\ c_n = b_n$. Получим

$$|f_n^*(t)| = |F_k(1)| \leqslant \left\{1 - |v(t)|^2 + |f_1(t)|^2 + 8\varphi(p)\right\}^{\frac{k}{2}} + 16\varphi(q)B_k, \tag{38}$$

где

$$B_k = \sum_{l=1}^{k-1} \left\{1 - |v(t)|^2 + |f_1(t)|^2 + 8\varphi(p)\right\}^{\frac{l-1}{2}}.$$

Пусть $|t| \leqslant \sigma_n(b_n)\sigma_p^{-1}(b_n) \sim \sqrt{k}$. С помощью леммы 2 получаем при достаточно больших $N > 0$

$$|f_1(t)|^2 - |v(t)|^2 = \frac{2t^2\sigma_q^2(b_n)}{\sigma_n^2(b_n)} - \frac{t^2\sigma_p^2(b_n)}{\sigma_n^2(b_n)} + o\left(\frac{t^2}{k}\right) \sim -\frac{t^2}{k}\left(1 - 2N^{-1}\right) + o\left(\frac{t^2}{k}\right) \leqslant -\frac{t^2}{2k}.$$

Подставив это неравенство в (30), выводим

$$|f_k(t)| \ll \exp\left\{-\frac{t^2}{4}\right\} + o\left(e^{-n^\varepsilon}\right).$$

Так как $b_n \sim \sigma_n(b_n)$, аналогичная оценка справедлива и для $f_n^*(t) = f_k\left(\dfrac{\sigma_n(b_n)}{b_n}t\right)$.

Доказательство теоремы 1. Прежде всего заметим, что

$$\left|\mathbf{P}\left\{\frac{T_n - n\mathbf{E}\xi_1(b_n)}{b_n} < x\right\} - \mathbf{P}\left\{\frac{T_n(b_n) - n\mathbf{E}\xi_1(b_n)}{b_n} < x\right\}\right| \leqslant$$

$$\leqslant 2\mathbf{P}\left\{\bigcup_{j=1}^{n}(\xi_j \neq \xi_j(b_n))\right\} \leqslant 2n\mathbf{P}\{|\xi_1| \geqslant b_n\} = 2\delta_n,$$

так что если обозначить

$$\Delta_n' = \sup_x \left|\mathbf{P}\left\{\frac{T_n(b_n) - n\mathbf{E}\xi_1(b_n)}{b_n} < x\right\} - \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} \exp\left\{-\frac{t^2}{2}\right\} dt\right|,$$

то будем иметь

$$|\Delta_n - \Delta_n'| \leqslant 2\delta_n. \tag{39}$$

Далее воспользуемся классическим неравенством Эссеена

$$\Delta_n' \leqslant \frac{1}{\pi}\int_{-T}^{T}\left|\frac{\chi(t)}{t}\right| dt + \frac{4}{\pi T}, \quad \chi(t) = f_n^*(t) - \exp\left\{-\frac{t^2}{2}\right\}$$

(см., например, [5, с. 119]), при $T = n^{\frac{1}{2}-\varepsilon}$. Получим

$$\Delta'_n \ll n^{-\frac{1}{2}+\varepsilon} + \int\limits_{|t|\leqslant n^{-1}} \left|\frac{\chi(t)}{t}\right| dt + \int\limits_{n^{-1}\leqslant|t|\leqslant\psi_n} \left|\frac{\chi(t)}{t}\right| dt + \int\limits_{\psi_n\leqslant|t|\leqslant n^{\frac{1}{2}-\varepsilon}} \left|\frac{\chi(t)}{t}\right| dt =$$

$$= n^{-\frac{1}{2}-\varepsilon} + I_1 + I_2 + I_3. \tag{40}$$

При $|t| \leqslant n^{-1}$ $|f_n^*(t) - 1| \leqslant t^2$, откуда легко получается

$$I_1 \leqslant n^{-2}. \tag{41}$$

I_2 оценим с помощью леммы 6:

$$I_2 \leqslant \int\limits_{n^{-1}\leqslant|t|\leqslant\psi_n} |t|^{-1}\Psi_2(t,n)\exp\left\{-\frac{t^2}{3}\right\} dt \ll \delta_n + \tau_n + n^{\frac{1}{2}-\varepsilon}. \tag{42}$$

Наконец, для оценки I_3 используем лемму 7:

$$I_3 \ll \int\limits_{\psi_n\leqslant|t|\leqslant n^{\frac{1}{2}-\varepsilon}} \frac{\exp\left\{-\frac{t^2}{4}\right\} + o\left(e^{-n^\varepsilon}\right)}{|t|} dt \ll \psi_n^{-2} + o\left(e^{-n^\varepsilon}\right) \leqslant \tau_n + o\left(e^{-n^\varepsilon}\right). \tag{43}$$

Из соотношений (39) – (43) следует утверждение теоремы.

Доказательство следствия 1.

Пусть $\mathbf{E}|\xi_1|^a < \infty$, $2 < a < 3$. Так как $\mathbf{E}\xi_1^2 < \infty$, то, как нетрудно видеть, $b_n^2 \sim \sigma_n^2 = \mathbf{D}T_n$. Из утверждения 1 леммы 2 следует, что $\sigma_n^2 \sim n\sigma^2$, где $\sigma^2 = \mathbf{E}\tilde{\xi}_1^2 + 2\sum\limits_{k=1}^{\infty}\mathbf{E}\tilde{\xi}_1\tilde{\xi}_{k+1} < \infty$, а из соотношения (2) $\sigma_n \to \infty$, $n \to \infty$, так что $\sigma > 0$. Имеем

$$\delta_n = n\mathbf{P}\{|\xi_1| \geqslant b_n\} \leqslant \frac{n\mathbf{E}|\xi_1|^a}{b_n^a} \ll n^{1-\frac{a}{2}}, \quad \tau_n = \frac{n\mathbf{E}|\tilde{\xi}_1(b_n)|^3}{b_n^3} \leqslant \frac{n\mathbf{E}|\tilde{\xi}_1|^a}{b_n^a} \ll n^{1-\frac{a}{2}}.$$

Из двух последних соотношений следует утверждение следствия 1.

Доказательство следствия 2.

Если $P\{|\xi_1| \geqslant x\} = \dfrac{h(x)}{x^a}$, $2 \leqslant a < 3$, где $h(x)$ — медленно меняющаяся функция, то

$$\mathbf{E}|\xi_1(x)|^a = -\int\limits_0^{b_n} x^3\, dP\{|\xi_1| \geqslant x\} \sim \frac{3-a}{a}x^3\mathbf{P}\{|\xi_1| \geqslant x\},\ x \to \infty$$

[11, с. 324]. Отсюда

$$\tau_n = \frac{n\mathbf{E}|\tilde{\xi}_1(b_n)|^3}{b_n^3} \ll n\mathbf{P}\{|\xi_1| \geqslant b_n\} = \frac{nh(b_n)}{b_n^a}$$

и при достаточно малых $\varepsilon > 0$

$$n^{-\frac{1}{2}+\varepsilon} \ll n^{1-\frac{a}{2}-\varepsilon} = o\left(\frac{nh(b_n)}{b_n^a}\right)$$

(см., например, вывод соотношения (29)). Утверждение следствия 2 следует теперь из Теоремы 1.

Литература

1. Гринь А.Г. Нормирующие последовательности в предельных теоремах для слабо зависимых величин // Теория вероятностей и её применения. 1991. Т. 36, № 2. С. 285–300.
2. Гринь А.Г. Об областях притяжения для сумм зависимых величин // Теория вероятностей и её применения. 1990. Т. 35, № 2. С. 255–270.
3. Hall P. Two-sided bounds for nonuniform rates of convergence in the central limit theorem // Z. Wahrscheinlichkeitstheorie verw. Geb. 1983. Bd. 65, N. 1. S. 61–72.
4. Тихомиров А.Н. О скорости сходимости в центральной предельной теореме для слабо зависимых величин // Теория вероятностей и её применения. 1980. Т. 25, № 4. С. 800–818.
5. Ибрагимов И.А., Линник Ю.В. Независимые и стационарно связанные величины. М. : Наука, 1965. 524 с.
6. Биллингсли П. Сходимость вероятностных мер. М : Наука, 1977. 351 с.
7. Сенета Е. Правильно меняющиеся функции. М. : Наука, 1983. 142 с.
8. Peligrad M. An invariance principle for φ-mixing sequences // Ann. Probab. 1985. V. 13, N. 4. P. 1304–1313.
9. Гринь А.Г. Уточнения центральной предельной теоремы для сумм зависимых случайных величин // Математические структуры и моделирование. 2003. Вып. 12. С. 10–27.
10. Лаврентьев М.А., Шабат Б.В. Методы теории функций комплексного переменного. М. : Наука, 1973. 736 с.
11. Феллер В. Введение в теорию вероятностей и её приложения. Т. 2. М. : Мир, 1984. 751 с.

Математические структуры и моделирование
2012, вып. 26, с. 20–37

УДК 51(091):929

ДЕЛО ЛУЗИНА — ТРАГЕДИЯ МАТЕМАТИКИ РОССИИ

С.С. Кутателадзе

Краткий обзор роли математиков в так называемом «деле академика Лузина» и анализ некоторых математических и гуманитарных корней этого исторического события.

Лузин и его ученики

Н.Н. Лузин

Николай Николаевич Лузин (1883–1950) — один из основоположников московской математической школы. Среди его учеников академики П.С. Александров (1896–1982), А.Н. Колмогоров (1903–1987), М.А. Лаврентьев (1900–1980), П.С. Новиков (1901–1975); члены-корреспонденты Л.А. Люстерник (1899–1981), А.А. Ляпунов (1911–1973), Д.Е. Меньшов (1892–1988), А.Я. Хинчин (1894–1959), Л.Г. Шнирельман (1905–1938) и многие другие математики.

В развитии математических исследований в Сибири выдающуюся роль сыграли прямые ученики Лузина М.А. Лаврентьев и А.А. Ляпунов, а также ученики А.Н. Колмогорова академики А.И. Мальцев (1909–1967) и А.А. Боровков.

Дело против Лузина

В 1999 году по математическому миру России прошло цунами — в книге [1] впервые были полностью приведены сохранившиеся с 1936 года в архивах канцелярии стенограммы заседаний печально известной чрезвычайной Комиссии Академии наук СССР по делу академика Лузина. Вскоре в США вышла в свет работа [2], отразившая воспоминания очевидца математических событий той поры в СССР профессора Г.Г. Лоренца (1910–2006)[1].

Комиссия «для разбора дела ак[адемика] Лузина» была создана Президиумом Академии наук СССР по следам статьи «О врагах в советской маске»,

Copyright © 2012 **С.С. Кутателадзе**

Институт математики им. С.Л. Соболева, Новосибирск
E-mail: sskut@math.nsc.ru

[1]Автор признателен В. Люксембургу, обратившему внимание на пропуск ссылки на работу [2] в предварительном варианте этой статьи.

появившейся в газете «Правда» 3 июля 1936 года. В ней Лузин обвинён во всех мыслимых для учёного грехах и нарисован врагом, сочетающим «моральную нечистоплотность и научную недобросовестность с затаённой враждой, ненавистью ко всему советскому». Он печатает «якобы научные статьи», «не стесняется выдавать за свои достижения открытия своих учеников», он недалёк от черносотенства, православия и самодержавия, «может быть, чуть-чуть фашистски модернизированных». Вот финальная часть этого пасквиля:

> Советская научная общественность срывает с вас маску добросовестного учёного и голеньким, ничтожным предстаёте перед миром вы, ратующий якобы за «чистую науку» и продающий интересы науки, торгующий ею в угоду прежним хозяевам вашим, нынешним хозяевам фашизированной науки. Советская общественность воспримет историю академика Лузина, как ещё один предметный урок того, что враг не складывает оружия, что он маскируется все искусней, что методы мимикрии его становятся все многообразней, что бдительность остаётся необходимейшей чертой каждого большевика, каждого советского гражданина.

Про статью в «Правде» и разгром «лузинщины» хорошо знали все учёные старшего поколения. Ни у кого не вызывало сомнений, что запуск кампании по дискредитации Лузина осуществлён симбиозом партийного и репрессивного аппарата СССР. За кулисами кампании маячили мрачные фигуры Э.Я. Кольмана (1892–1979) и Л.З. Мехлиса (1889–1953), типичных представителей опричнины той эпохи. Первый был в те годы заведующим Отделом науки Московского Комитета ВКП(б), а второй — главным редактором «Правды». Дело Лузина долгие годы рассматривалось всеми исключительно в контексте общих преступлений сталинского тоталитаризма.

Публикация архивных материалов выявила ранее скрытое обстоятельство — активными участниками политической травли Лузина выступили некоторые его ученики. Главную роль среди них при этом играл П.С. Александров, глава московской топологической школы.

С.П. Новиков пишет [3, с. 48]:

> Расследование было проведено тогда отцом (кажется, вместе с Люстерником и Лаврентьевым, знающим партийные круги). Они установили, что было письмо П. Александрова к влиятельному человеку по имени Хворостин[2], с возмущением излагающее мерзости Лузина. Хворостин находился в Саратове и имел большие связи в ЦК. Лузина он ненавидел, это было известно. Хворостин-то, как они решили, и передал материалы в ЦК и инициировал статью. Павел Сергеевич был великий мастер бильярдного удара!

Лузин особенно остро воспринимал инвективы П.С. Александрова, направленные на дезавуирование вклада Лузина в теорию аналитических множеств.

[2]Г.К. Хворостин (1900–1938) — математик по образованию, в 1935–1937 гг. был ректором Саратовского государственного университета. А.Я. Хинчин квалифицировал его как «партийную молодёжь» [1, с. 100].

Аналитическим множеством принято называть непрерывный образ борелевского подмножества числовой прямой. Эти множества часто связывают с именами Александрова и Суслина и называют A-множествами или суслинскими множествами[3]. Отметим, что на заседании комиссии 9 июля 1936 г. П.С. Александров говорит [1, с. 90]:

> Суслин назвал их A-множествами. Однако он никогда не говорил, что он назвал их так в мою честь.

В своих воспоминаниях 1979 г. он пишет прямо противоположное [6, с. 235]:

> Тогда же именно Суслин предложил назвать новую построенную мною теоретико-множественную операцию A-операцией, а множества, получающиеся её применением к замкнутым множествам, A-множествами. Он подчеркнул при этом, что предлагает эту терминологию в мою честь по аналогии с борелевскими множествами, которые уже тогда стало принято называть B-множествами.

Активное участие в заседаниях комиссии АН СССР принимали А.Н. Колмогоров, Л.А. Люстерник, А.Я. Хинчин, Л.Г. Шнирельман. Политическое нападение на Лузина энергично поддержали члены Комиссии С.Л. Соболев (1907–1989) и О.Ю. Шмидт (1891–1956). В защиту Лузина отважно выступали А.Н. Крылов (1863–1945) и С.Н. Бернштейн (1880–1968).

Последний пункт официального заключения Комиссии гласил [1, с. 296]:

> Все изложенное выше, резюмирующее многочисленный фактический материал, имеющийся в Академии наук, полностью подтверждает характеристику, данную Н.Н. Лузину в газете «Правда».

Все участники описанных событий 1936 года покинули этот мир. По всей видимости, они не знали о том, что стенограммы заседаний сохранились. Сейчас нам доподлинно во многих деталях известно происходившее как на Комиссии, так и вокруг неё. Математический мир очень болезненно переживает и переосмысливает роль учеников Лузина в организации его политической казни.

---

[3] С вопросом об открытии аналитических множеств связан таинственный эпизод, описанный незадолго до своей кончины А.П. Юшкевичем (1906–1993) [5]: В ходе наших довольно частых встреч во второй половине 70-х годов я не раз расспрашивал П.С. об истории открытия A-множеств. Как-то он позвонил мне и предложил приехать завтра к определённому часу, когда в его квартире останется он один. Я должен был войти в прихожую без звонка, а П.С. будет сидеть против двери на стуле. Так и получилось. Рассказ был долгий. Я записал его. На следующий день я привёз перепечатанный текст, и П.С. сказал, что он полностью соответствует им сказанному, и тут же поставил условие: не публиковать запись при его жизни. Когда в 1982 г. П.С. скончался, я решил спросить совет у А.Н. Прослушав текст, А.Н. сказал, что печатать его слишком рано. Теперь нет ни П.С., ни А.Н., и больше советоваться мне не с кем. Я решил запечатать рассказ П.С. Александрова в конверт и сдать в таком виде на хранение в Архив АН СССР в фонд П.С. Александрова с надписью: «Получено от А.П. Юшкевича. Разрешается вскрыть через 10 лет после его смерти».

Ж.-М. Кантор сообщил, что его попытки, как и попытки С.С. Демидова, обнаружить этот конверт в Архиве РАН оказались безрезультатными. (**С.К.**)

Роль учеников Лузина

В публичной травле Лузина не замечены ни П.С. Новиков, ни М.А. Лаврентьев (хотя оба фигурировали на Комиссии в числе обкраденных Лузиным). Теперь становится понятным, почему к 90-летию Лузина статью [7] о нем для «Успехов математических наук» М.А. Лаврентьев написал единолично и включил в свою книгу общенаучных публикаций [8]. Он же возглавил редакционную коллегию трудов Лузина, изданных по решению АН СССР уже после кончины Лузина к 70-летию со дня его рождения. Ни П.С. Александров, ни А.Н. Колмогоров в эту редколлегию не вошли[4].

Разъяснения своих отношений с Лузиным, которые при жизни оставили П.С. Александров и А.Н. Колмогоров, по сути, одинаковы. Высказанные ими суждения по сей день в той или иной форме разделяются их многочисленными учениками. Подчёркивается, что Лузин был не таким значительным математиком, как затравившие его ученики. Лузину особо настойчиво инкриминируется некоторая моральная вина в ранней смерти М.Я. Суслина (1894–1919) от тифа. Нередко говорят, что Лузин сам виноват во всех своих бедах, хотя бы отчасти. Ему приписывают такие черты, как театральность, двуличие, беспринципность, зависть к чужим успехам, плагиаризм и склонность к интриганству[5]. Считается, что Лузин получил по заслугам, а если и не только по заслугам, то не от учеников, а от сталинщины или времени. Это суждение разделяют не только пожилые, но и многие молодые люди. В лучшем случае, они с сожалением считают дело Лузина общей трагедией всех его участников.

Между тем надо отличать личную трагедию Лузина от трагедии не только московской, но и всей отечественной математики. Сами ученики Лузина, участвовавшие в травле своего учителя, вовсе не считали свою судьбу трагичной.

В своих воспоминаниях П.С. Александров писал [6, с. 242–243]:

> Узнав Лузина в эти самые ранние творческие его годы, я узнал действительно вдохновенного учёного и учителя, жившего только наукой и только для неё. Я узнал человека, жившего в сфере высших человеческих духовных ценностей, в сфере, куда не проникает никакой тлетворный дух. Выйдя из этой сферы (а Лузин потом вышел из неё), человек неизбежно подпадает под власть тех сил, о которых Гёте сказал:
>
> Ihr fuhrt in's Leben uns hinein,
> Ihr lasst den Armen Schuldig werden
> Dann uberlasst Ihr ihn der Pein,
> Denn jede Schuld racht sich auf Erden.

[4] О взаимоотношениях Лузина и М.А. Лаврентьева немного сказано в воспоминаниях М.М. Лаврентьева [9, с. 45–47].

[5] Человек с подобными изъянами личности не мог стать основателем «Лузитании» — самой успешной научной школы в математике. Поэтому бытует не лишённая оснований теория «двух Лузиных» — эпохи Лузитании и эпохи дела Лузина.

Вы вводите нас в жизнь,
Вы делаете беднягу виновным.
Потом вы предаёте его на муку,
Потому что на земле отмщается всякая вина.

Лузин в последние годы своей жизни до дна испил горькую чашу отмщения, о котором говорит Гёте[6].

Стоит отметить, что А.Я. Хинчин, враждебно относившийся к Лузину, так комментировал обвинения в доведении М.Я. Суслина до смерти [10, с. 391]:

Суслина называют учеником Н.Н. Лузина, загубленным Н.Н. Ну, когда человек умирает от сыпного тифа, то это слишком резкое выражение. Ведь он мог заболеть сыпным тифом и в Иванове. Но общее мнение таково, что из Иванова Н.Н. выжил Суслина. Однако самый перевод из Москвы в Иваново я считаю услугой, оказанной Суслину Н.Н., тогда ещё не враждебно настроенному по отношению к Лузину.

Диктуя свои воспоминания о П.С. Александрове, А.Н. Колмогоров сказал в 1982 году [11, с. 7]:

Вся моя жизнь в целом оказалась преисполненной счастья.

Ни он, ни П.С. Александров, ни другие участники травли Лузина не считали дело Лузина общей с Лузиным трагедией. Они были правы в таком суждении, но совсем не по тем причинам, что декларировали.

Если у Лузина и была вина, она лежала в сфере камеральных математических отношений учитель-ученик. Сколь-либо убедительных доказательств плагиаризма Лузина не предъявлено. Инкриминируемые ему обвинения в приписывании А. Лебегу (1875–1941) или присвоении себе результатов М.Я. Суслина шиты белыми нитками и грубо натянуты.

Как доказательство научной недобросовестности Лузина фигурировал и тот факт, что Лузин якобы из низкопоклонства и лести аттрибутировал А. Лебегу свой собственный метод решета. Сам же А. Лебег писал в предисловии к книге Лузина [12]:

Всякий, вероятно, удивится, когда узнает, читая Лузина, что я, между прочим, изобрёл метод решета и первым построил аналитическое множество. Никто, однако, не удивится так, как я. Г-н Лузин лишь тогда бывает совершенно счастлив, когда ему удаётся приписать собственные открытия кому-либо другому.

[6] П.С. Александров цитирует стихотворение *Harfenspieler*, датированное 1795 годом, и даёт его подстрочный перевод. Известен перевод этих строк, принадлежащий Ф.И. Тютчеву:

Они нас в бытие манят —
Заводят слабость в преступленья —
И после муками казнят:
Нет на Земле проступка без отмщенья!

Ученики были явно «святее папы»[7].

Как бы то ни было, нельзя не констатировать своего рода конфликт поколений — пропасть отчуждения и непонимания между Лузиным и наиболее успешными из его учеников. Легко допустить подлинную или кажущуюся несправедливость и предвзятость Лузина в цитировании учеников и подлинную или мнимую слабость Лузина в преодолении математических трудностей. Можно признать двуличие в решении не голосовать за П.С. Александрова на академических выборах вопреки личному письму к А.Н. Колмогорову о поддержке П.С. Александрова. Но разве в этом есть из ряда вон выходящее или нетипичное для академических нравов? Разве из этого что-то серьёзное или трагическое следует? Разве в этом суть дела Лузина?

Нам известно свидетельство выдающегося польского математика В. Серпинского (1882–1969), объявленного «махровым черносотенцем» на заседаниях Комиссии по делу Лузина [13, с. 124]:

> В своем письме от 27 июля 1935 г. — то есть вот уже год назад — г-н Лузин писал: «Возвращаясь теперь к очень трудной для меня самозащите по поводу приписывания Суслину тех результатов, на которые он не имел никакого права и которых у него даже в мыслях не было, я должен сказать, что эта самозащита спровоцирована очень большой и совершенно реальной опасностью. Г-н Александров имеет виды войти в Академию наук в качестве действительного члена, сместив меня. С этой целью он требует пересмотра моих работ, заявляя, что я не имею права быть членом Академии, поскольку мои идеи все украдены у Суслина. Такой пересмотр вполне возможен и реален». Когда я был в Москве, в сентябре 1935 г. г-н Александров заверил меня, что опасения Лузина — чисто мнимые и что он очень уважает Лузина, своего бывшего учителя. В моем присутствии Александров протянул руку Лузину и объявил, что всегда будет его другом.

Разве притворное примирение П.С. Александрова с Лузиным, которое описывает В. Серпинский и от которого потом П.С. Александров публично открещивается, никак не похоже на отказ Лузина поддерживать П.С. Александрова при выборах в академики? Считается, что именно за этот поступок А.Н. Кол-

[7] Вот соответствующий фрагмент стенограммы от 13 июля 1936 г. [1, с. 196–197]:

> **Александров.** Что касается низкопоклонства, то я предлагаю тут сказать устами самого Лебега: (читает по-французски). По этому поводу я имею объяснения, которые я готов мотивировать как угодно. Вот эта «странная мания», я бы сказал, — глубоко продуманная идея. Он приписывает Лебегу свои вещи, приписывает столь нелепым образом. Ни один разумный человек не станет их приписывать Лебегу. Но этим он создаёт себе репутацию человека, который даже свои идеи приписывает другому, и когда дело идёт об его собственных учениках, то он под этой ширмой присваивает себе их вещи.
>
> **Люстерник.** Эта защита была как раз на нашем собрании, в нашем Институте, явно им инспирированная защита, именно на этом основании: как это Н.Н. присваивает чужие результаты, если даже Лебег о нем так пишет?
>
> **Александров.** Это низкопоклонная система, потому что в научных кругах не принято приписывать своих результатов другим. Так что здесь мы имеем, с одной стороны, угодливость перед Лебегом, а с другой стороны, создание ширмы, которая позволяет ему действовать таким образом.

могоров в 1946 году дал публичную пощечину Лузину[8].

Л.С. Понтрягин пишет 24 декабря 1946 г. [16, Письмо №49, с. 89–91]:

> Вы интересуетесь совместной работой Колмогорова и Лузина. Это, конечно, нужно рассказывать, а не писать, так как требуется выражение голоса, чтобы передать все. Летом Колмогоров сказал мне, что единственное его беспокойство относительно избрания Александрова заключается в том, что он стал несомненным кандидатом за четыре месяца до выборов. Пусики[9] провели большую подготовительную работу в смысле установления всяких соглашений с академиками. Виноградову, например, было обещано, что Колмогоров будет поддерживать Лаврентьева за то, что Виноградов поддержит Александрова. В общем, казалось, что все будут за Александрова. Бернштейн, например, на заседании института сам выдвинул кандидатуру Александрова, правда и Чеботарева тоже. Колмогоров договорился с начальством, что его включат в экспертную комиссию. Первой тревожной вестью было то, что его не включили, но он надеялся, даже был уверен, что это уж не важно. После работы экспертной комиссии произошло несколько закрытых совещаний академиков по обсуждению кандидатов, и тут только Колмогоров узнал, что ни один из членов экспертной комиссии не поддерживает Александрова. Бернштейн, напротив, яростно против него возражает, говоря, что у Александрова вредное направление. Поведение Бернштейна кажется мне до сих пор мало понятным, быть может, он просто поругался с Пусиками. Все остальное довольно понятно. Лаврентьев оказался почему-то бесспорным кандидатом и не нуждался в поддержке Колмогорова, который и в комиссию-то не входил. Таким образом, Виноградов вовсе не нуждался в Колмогорове и Пусике. Что же касается Соболева, и Христиановича, то первый чрезвычайно ненавидит Пусика за изгнание из директоров, второй же — его друг и приятель. При сложившейся обстановке надежды на успех почти не было. Оставалась только возможность, что некоторые из академиков-математиков поддержат Александрова, физики его поддержать хотели, но, конечно, не могли идти против всех математиков. Лузин стал надеждой Пусиков, он был ими приглашен в Комаровку и обещал поддержку. Однако на окончательном закрытом совещании выступил против Александрова. По выходе с этого совещания совершенно расстроенный и обозлённый Колмогоров подошёл к Лузину и сказал, что не может теперь иметь с ним ничего общего. Лузин же сделал вид, что ничего не понимает, и стал говорить так: «Голубчик, успокойтесь, да что с Вами, да Вы больны, успокойтесь». Вот это нужно было рассказывать с выражением. Колмогоров тогда сказал ему: «Ну что же мне с Вами делать, в физиономию Вам плюнуть или по морде дать» Подумав, он решился на последнее»[10].

[8]Относительно версий этого эпизода см. недавнюю монографию Л. Грэхема и Ж.-М. Кантора [14, p. 186], воспоминания С.М. Никольского [15, с. 155] и С.П. Новикова [3, с. 22].

[9]Для англоязычного читателя слово «Пусики» имеет скабрезную коннотацию, отсутствующую в русском языке.

[10]Выборы в 1946 году состоялись 30 ноября. По Отделению физико-математических наук на вакансии академиков по специальности «математика» были избраны М.А. Лаврентьев и И.Г. Петровский (1901–1973). Членами-корреспондентами стали А.Д. Александров (1912–

В.М. Тихомиров приводит переписку Лузина с А.Н. Колмогоровым о выборах П.С. Александрова. Осенью 1945 г. Лузин пишет А.Н. Колмогорову [10, с. 80]:

> Теперь о другом: приближается время выборов в Академию. Было бы абсолютной несправедливостью, если бы они протекали без Павла Сергеевича. Его работы, отзвуки которых всюду в мировой литературе, его прекрасные зрелые годы — полнота зрелости — разума — и он сам, интереснейший муж, — всё это заставляет видеть в нем достойного кандидата, польза активности которого для Академии неоценима.

А.Н. Колмогоров переоценивает позицию Лузина, который ни слова не пишет о том, что будет поддерживать П.С. Александрова иначе как в качестве кандидата для избрания (что им было выполнено).

В ответном письме от 7 октября 1945 г. [10, с. 82] А.Н. Колмогоров отмечает:

> Так как я уже ряд лет занят тем, чтобы различные случайные и привходящее обстоятельства не помешали бы ещё раз вполне справедливому, на мой взгляд, избранию Павла Сергеевича, то я действительно очень ценю Вашу готовность тогда, когда это действительно оказывается нужным, поддержать необходимые для успеха действия.

Таким образом, А.Н. Колмогоров без достаточных к тому оснований решил, что Лузин будет поддерживать не выдвижение П.С. Александрова, а его избрание. Между тем ничего такого ему в письме Лузин не обещает. По давней традиции номинирование и избрание в Академии наук, как и в других выборных институтах, — процедуры достаточно независимые.

Принято считать, что А.Н. Колмогоров был спокойным и не склонным к вспышкам и срывам. Поэтому для пощёчины ему нужна была особая провокация со стороны Лузина и здесь фигурируют апокрифы о неприличной реплике со стороны Лузина на выборах 1946 г.[11]. Между тем ученики А.Н. Колмогорова отмечают иные малоизвестные особенности его личности.

В.М. Тихомиров пишет [11, с. 83]:

> ...надо сказать, что в характере Колмогорова была одна болезненная особенность: иногда он терял власть над собой.

В.И. Арнольд свидетельствует [17, с. 50]:

> Андрей Николаевич никогда не был слишком добронравным и не без гордости рассказывал о своей драке с милицией на Ярославском вокзале.

1999), Н.Н. Боголюбов (1909–1992), Л.А. Люстерник и В.В. Степанов (1889–1950).

[11]См., в частности, [12, p. 186; 3, с. 22]. Аналогичную версию упоминал в частной переписке В.И. Арнольд (1937–2010). Не исключено, что бытующие намёки на «тоположство» — продукт 1950 годов, пущенный для реабилитации зачинщиков «дела Лузина».

Лузин на двадцать лет старше А.Н. Колмогорова. Лузин — учитель А.Н. Колмогорова, с которого не сняты политические обвинения, навешанные при участии П.С. Александрова и А.Н. Колмогорова. Лузин был «прощён» и принят на даче у А.Н. Колмогорова и П.С. Александрова перед выборами[12]. Разве кто-то из участников встречи в Комаровке не помнил главного — Лузин повержен и должен подчиняться благородным победителям? Разве это не видно теперь? Разве можно ставить внутринаучные отношения и, допустим, некорректное поведение Лузина и даже его плагиат, в один ряд с обвинениями во вредительстве и антисоветчине? Горькие и тяжёлые вопросы...

Заключая заседание 13 июля 1936 г., председатель Комиссии Г.М. Кржижановский (1872–1959) сказал, в частности [1, с. 198]:

> А затем нам нужно подумать о следующем. Осенью будут выборы, и нам дают понять, что нужно будет выбрать 30 новых академиков и 60 новых членов-корреспондентов. Нам нужно освежить состав, и Вы должны подумать к сентябрьской сессии — кого Вы рекомендуете ввести в состав членов-корреспондентов и академиков. Это будет самый лучший результат работы Комиссии.

В 1936 году выборы в Академию не были проведены. Большие выборы состоялись только 29 января 1939 года (см. [23, № 241, 242]). По Отделению математических и естественных наук академиками были избраны А.Н. Колмогоров и С.Л. Соболев, а членами-корреспондентами А.О. Гельфонд (1906–1968), Л.С. Понтрягин (1908–1988) и А.Я. Хинчин.

Реакция современников на дело Лузина

Моральные обвинения против Лузина малообоснованны. То, что предъявляется как доказательства, таковыми не были даже в то время ни для П.Л. Капицы (1894–1984), ни для В.И. Вернадского (1863–1945), ни для А. Данжуа (1884–1974), ни для А. Лебега, ни для многих других людей, достигших зрелого возраста.

Возражения П.Л. Капицы сформулированы 6 июля в письме Председателю Совета Народных Комиссаров СССР В.М. Молотову[13]. На следующий день В.И. Вернадский пишет в своих дневниках [18, с. 92]:

> Письма Лузину, Чаплыгину и Ферсману о нём. Многие принимают как доказанную эту клевету и инсинуации. М[ожет] б[ыть], он [нужен] за границей, а не здесь. Боюсь, что эта безобразная статья сильно на него подействует. Много разговоров и много впечатлений.

[12] О встрече в Комаровке В.М. Тихомиров пишет: «Из переписки Л.С. Понтрягина с его учеником и другом И.И. Гордоном выясняется, что Лузин был даже зван и потчуем в Комаровке» [10, с. 83].

[13] Недавно выяснилось, что это письмо было размножено в 16 экземплярах для членов Политбюро ВКП(б) и обсуждено вместе с другими письмами в защиту Лузина.

В тот же день им послано письмо на имя члена Комиссии А.Е. Ферсмана (1883–1945), в котором В.И. Вернадский отмечает [17, с. 94]:

> Я думаю, что подобная история может оказаться, в конце концов, гибельной для Академии, если она приведёт к удалению Н.Н. [Лузина] из Академии или чему-нибудь подобному. Мы покатимся вниз по наклонной плоскости.

А 11 июля С.А. Чаплыгин (1869–1942) пишет В.И. Вернадскому [19, с. 106–107]:

> Статья о Лузине прямо возмутительна: пусть он погрешил в оценке того или другого претендента на учёную степень, учёное звание; но как отсюда делать выводы о вредительстве?! ... Что касается обвинений в фашизме, проскальзывающих в статье, в принадлежности к старой московской реакционной школе математиков, то я этого уже совсем не понимаю. Остаётся критическая оценка работ Лузина. Но по этому поводу приходится сказать только то, что здесь вполне обнаружилась полная несостоятельность авторов, доказывающая малое и поверхностное знакомство с его работами, их сознательное искажение правильной оценки. Авторитет его несравним с авторитетом Хинчина, который ему противопоставляется. Но что теперь делать? Как помочь Н.Н.? Я сделал пока одно: послал телеграмму Н.Н., копию которой прилагаю: «Поражён неожиданными совершенно незаслуженными газетными нападками на Вас. Ваш высокий всемирно признанный научный авторитет не может быть поколеблен. Твёрдо надеюсь, что Вы найдёте в себе силы спокойно отнестись к малоавторитетной критике Ваших трудов. О совершенно необоснованных обвинениях другого порядка не говорю».

Вот письмо от 5 августа 1936 года А. Лебега, избранного в 1929 году за выдающийся вклад в математику в Академию наук СССР. Великий Лебег, автор того самого «интеграла Лебега», без которого нет современной математики, взбешён до крайности и пишет [11, с. 127]:

> Вы увидите, что нападки на Лузина с целью его изгнания и освобождения места для Александрова, начались не вчера. Вы увидите там, что меня уже приписали к этому, противопоставляя «мою» науку, буржуазную и бесполезную, analysis situs [топологии], пролетарской и полезной науке. Потому что первая была наукой Лузина, а вторая — наукой Александрова. Что любопытно, так это то, что Александров исходит, как это делал Урысон, бумаги которого унаследовал Александров, из той же отправной точки, которая была и моей. Только с той разницей, что Урысон ссылался на меня, а Александров больше на меня не ссылается, так как он теперь должен плохо отзываться обо мне в своей борьбе против Лузина!

А вот ещё одно свидетельство В. Серпинского [11, с. 125]:

> Я придерживаюсь того мнения и того же мнения мои польские коллеги, что присутствие господ Александрова, Хинчина, Колмогорова, Шнирельмана, которые самым нечестным образом выступили против своего бывшего учителя и ложно обвинили его, — нельзя терпеть ни в каком собрании честных людей.

Метод политических обвинений и клеветы был использован против старой московской профессуры много раньше статьи в «Правде». В декларации «инициативной группы» Московского математического общества от 21 ноября 1930 года в составе Л.А. Люстерника, Л.Г. Шнирельмана, А.О. Гельфонда, Л.С. Понтрягина и К.П. Некрасова указано (см. [10], [20]):

> Обострившаяся классовая борьба в СССР толкнула правую часть профессуры в лагерь контрреволюции. Реакционная профессура возглавляла все раскрытые в последнее время вредительские организации и контрреволюционные партии. Благодаря блестящей деятельности ОГПУ разоблачены преступления целого ряда научных бонз, умевших искусно скрываться за разными масками — от холодной лояльности до шумно рекламируемой горячей привязанности к советской власти. И в среде математиков выявились активные контрреволюционеры. Арестован за участие в контрреволюционной организации профессор Егоров, признанный вождь Московской математической школы, председатель Математического общества, бывший директор Математического института, кандидат московской математики в Академию наук, — тот самый Егоров, хранитель академических традиций, против которого уже давно велась борьба пролетарским студенчеством, но в защиту которого почти единогласно выступало общество московских математиков.

Д.Ф. Егоров (1869–1931) — учитель Лузина. После ареста Д.Ф. Егорова Лузин счёл за благо покинуть университет (в чем потом был также обвинён учениками).

В своём жизнеописании, датируемом концом 1970 годов, Л.С. Понтрягин отмечал [21, с. 91]:

> Два моих выступления — в 1936 году по поводу Лузина и в 1939 году по поводу выборов — являлись важными этапами становления меня как общественного деятеля. В моем понимании оба они были борьбой за правое дело.

Как не сочетается это с позицией Лузина, который уже после дикой декларации с участием А.О. Гельфонда сообщает в своём письме 1934 года Л.В. Канторовичу (1912–1986), что при выборах в члены-корреспонденты Академии наук по Москве будет «стоять за Гельфонда, сделавшего недавно гениальное открытие» [22]. А в 1939 году Лузин пишет В.И. Вернадскому (см. [19, с. 105]):

> Владимир Иванович, кандидаты по математике — Соболев и Колмогоров — хорошие. Я буду голосовать за них.

В 1936 году по стране прокатилась широкая кампания осуждения Лузина и «лузинщины» [23, с. 757–767]. К счастью, Лузин не был ни репрессирован, ни исключён из Академии. По мнению некоторых историков, на сей счёт последовало устное указание И.В. Сталина. Однако ярлык врага в советской маске Лузин носил 14 лет до самой смерти. Изуверство, учинённое над Лузиным, не идёт ни в какое сравнение с предъявленными ему этическими претензиями.

Математические корни дела Лузина

Очевидны людские страсти и заблуждения — любовь и ненависть, зависть и восхищение, тщеславие и скромность, бескорыстие и карьеризм, ставшие внутренними пружинами трагедии отечественной математики в тридцатые годы прошлого столетия. Но были ли у этой трагедии математические причины? Некоторые корни такого рода бросаются в глаза.

Нам дарован чудесный мир, обладающий бесспорным свойством единственности. Уникальность сущего воспринималась нашими пращурами как безусловное доказательство единственности мира. Именно этим обстоятельством можно объяснить неустанные многовековые попытки доказательства пятого постулата Евклида. На том же основано и общее желание найти единственное наилучшее решение любой человеческой проблемы.

Математика никогда не могла освободить себя от тенет экспериментальности. И дело не просто в том, что мы до сих пор завершаем математическое доказательство ссылкой на очевидность. Живы и весьма популярны воззрения на математику как на набор технических средств естествознания. Такие взгляды можно выразить лозунгом «математика — это экспериментальная теоретическая физика». Не менее распространено и двойственное суждение: «теоретическая физика — это экспериментальная математика». Наше краткое отступление подчёркивает тесную взаимосвязь течения мысли в математике и естественных науках.

Стоит отметить, что догматы веры и принципы теологии также нашли хорошее отражение в истории математических теорий. Вариационное исчисление было изобретено в поисках лучшего понимания принципов механики, основанных на религиозных воззрениях об универсальной красоте и гармонии акта творения.

XX век отмечен важным изменением в содержании математики. Математические идеи впитались в гуманитарную сферу и прежде всего в политику, социологию и экономику. Общественные явления принципиально изменчивы и обладают высокой степенью неопределённости. Экономические процессы связаны с широким диапазоном возможных способов организации и управления производством. Яснее ясного природа неединственности в экономике: подлинные интересы различных людей не могут не противоречить друг другу. Единственное решение — это оксюморон в любой мало-мальски нетривиальной проблеме экономики, связанной с распределением благ между многими агентами. Далеко не случайно то, что социальные науки и другие проявления гуманитарной ментальности связаны с многочисленными гипотезами, касающимися наилучшей

организации производства и потребления, наиболее справедливой и правильной социальной структуры, с кодификацией рационального поведения и моральных принципов, et cetera.

Двадцатое столетие стало веком свободы. Плюрализм и единственность противостояли друг другу как коллективизм и индивидуализм. Многие конкретные проявления жизни и культуры отражают такие различия. Ликвидация монархизма и тирании сопровождалась подъёмом парламентаризма и демократии. Квантовая механика и принцип неопределённости Гейзенберга воплотили плюрализм в физике. Стоит вспомнить волны модернизма в поэзии и живописи. Человечество изменило все пределы своего обитания и мечты.

Поиск плюрализма в математике привёл к отказу от всеобщего давления единственности и категоричности. Последние идеи практически отсутствовали или были периферийными в Древней Греции. Они воспряли с расцветом абсолютизма и христианства. Г. Кантор (1845–1918) стал предвестником грозных перемен, заявив, что «сущность математики заключена в её свободе». Как это ни парадоксально, воскрешение свободы изгнало математиков из канторовского рая.

Сегодня мы привыкли к неразрешимости или алгоритмической неразрешимости многих проблем. Для нас не составляет большой сложности принять нестандартные модели и разные версии модальной логики. Нас не смущает неразрешимость проблемы континуума в рамках теории множеств Цермело — Френкеля. Какими бы элементарными не казались эти взгляды сегодня, они представлялись совершенно оппортунистическими и противоречивыми во времена Лузина. Успешные прорывы в науке, осуществлённые великими учениками Лузина, были основаны на отказе от его математических идей. Таково психологическое, отчасти фрейдистское обоснование дела Лузина. Его одарённые ученики чувствовали необходимость освобождения от дескрипции и сопутствующих чудесных, но неосуществимых мечтаний Лузина с целью достижения математической свободы. Его ученики пошли по ложному пути и сознательно или бессознательно трансформировали благородное стремление к свободе в примитивные ненависть и жестокость. Подобное преобразование было и остаётся пунктиком и хобби людей.

Ужасно и нестерпимо легкомысленное всеобщее удовольствие, состоящее в возложении на Лузина вины за преступления в математике, которые он вряд ли совершал, с едва скрытым намерением отомстить Лузину за его мнимые и подлинные личные грехи. Стоит понять, что идеи дескрипции, финитизма, интуиционизма и других подобных героических предприятий начала XX века по поиску единственного верного и последнего обоснования были неизбежны на пути освобождения математики от иллюзий категоричности. Коллапс вечной единственности и абсолютизма стал триумфом и трагедией математических идей первых двух десятилетий прошлого века. Расцвет творческих идей учеников Лузина проистекал отчасти из его математических иллюзий в дескрипции.

Борьба против Лузина имела математические корни, которые было невозможно извлечь и объяснить в то время. Теперь мы ясно видим, что эпоха теории вероятностей, функционального анализа, обобщённых функций и топо-

логии началась тогда, когда идея единственного последнего обоснования была разрушена раз и навсегда. К. Гёдель (1906–1978) указал некоторые особенности мышления, объясняющие данный феномен, но совершенные математики чувствовали их, руководствуясь врождённой интуицией и вызовами разума.

Видение современной московской школы началось с Лузина. Лузин интересовался основаниями, и дескрипция для него была методом понимания математики в целом. Возникнув как теория измеримости, дескрипция не умерла — она жива в рекурсивном анализе и других идеях, связанных с вычислимостью и тезисом Чёрча.

Дескрипция играет такую же роль по отношению к финитизму и интуиционизму, как абсолютная геометрия по отношению к эллиптической и гиперболической. Процедуры и идеология дескрипции — предтечи идей вычислимости и алгоритма. Творчество А.Н. Колмогорова в теории алгоритмов, вычислимости, сложности — компонента, выросшая из дескрипции. Теория вероятностей, турбулентность, анализ — компонента, выросшая из отказа от дескрипции. Математика не сводится ни к финитизму, ни к интуиционизму, ни к дескрипции. Она не категорична, она свободна. Эту свободу математики в России лучше других демонстрировал в XX веке А.Н. Колмогоров, ученик Лузина и учитель новых поколений отечественных математиков. Он был более свободен в математике и, значит, был бóльшим математиком.

Трагедия математики в России состоит в том, что благородное стремление к свободе породило политическое изуверство гигантов науки, облачённых в рясы Торквемады.

Некоторые уроки

История и ушедшие люди неподсудны. Учёные и просто люди обязаны констатировать факты. Не осуждать ушедших, а спокойно и прямо указывать на то, что было. Разъяснять молодым отличие моральных обвинений от политических инсинуаций и клеветы. Объяснять трудность и необходимость исправления ошибок и покаяния. Показывать, как легко прощать себя и винить других.

Мы обязаны формировать в себе и передавать другим объективный взгляд на прошлое. На его успехи и трагедии. С любовью и сомнениями, с пониманием несчастной нашей судьбы и с честью объективности. Осуждать и исправлять стоит, прежде всего, собственные ошибки и промахи. Ещё в Древнем Риме понимали, что о мёртвых пристало либо ничего не говорить, либо говорить хорошее. Факты мёртвыми не бывают. Лузина осудили и Академия наук и московская математическая общественность.

Защита сталинщины часто состоит в том, что делается вид, будто в её мерзостях виноваты только сталины, берии, мехлисы и кольманы, а на самом деле создавали сталинщину миллионы. Сталинщину в науке в огромной мере порождали учёные. Делать вид, что ученики Лузина спасали своего учителя и науку от сталинщины, неприлично. Лузин был подвергнут социальному остракизму и четырнадцать лет до самой смерти жил с клеймом врага в советской маске. Для сталинщины он стал показательным социальным изгоем — враг, а

на свободе. Коллеги и ученики Лузина унижали, дело дошло до рукоприкладства и плевка на его могилу. Лузина нет, а ложные обвинения от коллег на него во вредительстве и низкопоклонстве есть.

Нельзя забыть слова Лузина [1, с. 73]:

> Что касается последнего абзаца статьи «Правды», где мне предъявляются чудовищные обвинения в прислуживании нынешним хозяевам фашизированной науки, то я с полным сознанием своей политической ответственности, как учёного с мировым именем и гражданина Союза, заявляю, что редакция «Правды» была сознательно введена в заблуждение людьми, заявившими ей об этом. Это опровергается всей моей жизнью и деятельностью, как учёного и как человека.
>
> Я не нахожу слов, способных выразить всю глубину моего негодования по поводу предъявления мне обвинения в «прислуживании хозяевам фашизированной науки». При всех моих ошибках и заблуждениях я никогда не испытывал иного чувства, как чувство мерзостного отвращения к разрушителям науки, служению которой я посвятил всю свою творческую жизнь.

Любые попытки увидеть нравственное в безнравственном прошлом опасны тем, что эту самую безнравственность и питают, создавая ей комфортную среду в настоящем и будущем. Свойство быть учёным по убеждениям — разрывная функция времени. Наука не прививает нравственность. Злодейство и гений вполне уживаются в различные моменты.

История не просто раздел науки, а предмет ответственности настоящего. Наука и совесть взаимосвязаны. История не существует без людей. Никому не дано изменить исторические события, но человечество — не сторонний наблюдатель прошлого. Прошлое — это прошлое настоящего, а, значит, предмет ответственности сегодняшнего дня. Живые, а не мёртвые, отвечают за прошлое. Это мы меняем настоящее и тем создаём будущее. История будит нашу совесть и стучит в наши сердца как пепел Клааса стучал в сердце Тиля Уленшпигеля.

Эпилог

Президиум РАН 17 января 2012 г. поставил точку в «деле Лузина», отменив позорное Постановление Президиума АН СССР от 5 августа 1936 г.

Инициаторами дезавуирования позорных решений выступили академики А.А. Боровков, В.Е. Захаров, И.А. Ибрагимов, В.Е. Накоряков, А.К. Ребров и Ю.Г. Решетняк, обратившиеся прошлым летом с письмом к руководству РАН. Идею реабилитации Лузина разделяли многие учёные нашей страны. Среди них академики А.Г. Аганбегян, В.И. Арнольд, Р.И. Нигматулин, Я.Г. Синай, Д.В. Ширков и другие учёные. Обращение, инициированное в Сибири, поддержали в Отделении математических наук РАН. Были и противники идеи, главным аргументом которых служила ссылка на срок давности — судилище над Лузиным состоялось в Академии наук СССР 75 лет назад.

Источники «дела Лузина» не локализованы в каких-то специальных тоталитарных механизмах 1930-х годов. Сменились формации России, но и по сей день многие считают, что с Лузиным поступили справедливо, ибо он хуже математик, чем его ученики. Карьеризм, попустительство, сотворение кумиров из собственных учителей и начальников — вещи более чем заурядные. Мало удовольствия убеждаться в том, что великие учёные и благоверные святые могут быть злодеями, но скрывать неприятные факты не объективно. Такие случаи особо поучительны, как свидетельствует история. Библия рассказывает нечто подобное.

Исторический нигилизм служит нигилизму нравственному. «Прошлые преступления канули в прошлом. Прошлого нет сейчас. Значит, сейчас нет и прошлых преступлений. А на нет и суда нет». Этот софизм лежит в основе лукавого призыва игнорировать прошлые проявления субъективизма, монополизма, протекционизма и даже измов покруче. Последнее дело ссылаться на сроки давности в вопросах науки, нравственности и морали. Там их просто нет. Срок давности ни одной ошибки не элиминирует — исчезают ошибки только исправленные. Делать ошибки легче, чем их исправлять. Ещё труднее исправлять ошибки чужие и прошлые. Когда это удаётся, ошибок становится меньше. От ошибок прошлого надо отмежёвываться, искоренять их причины и исправлять их последствия, а не прятаться за фальшивым аргументом срока давности. Позиции наших дней по Катыни и «делу Лузина» — символы неистребимой российской душевной чуткости и совестливости в политике и в науке.

«Дело Лузина» 75 лет наносило ущерб престижу отечественной науки, отравляло жизнь ложью, замалчиванием мерзостей прошлого, вольным или невольным оправданием политических доносов, конъюнктурных расправ, давления, подножек и прочих средств зачистки карьерного поля. Этому положен конец — в науке стало немного чище. Лузин о нас не узнает, но память его станет ярче, а путь молодых в науке светлее. Честь Лузина — часть личной чести многих учёных. Честь российской науки не умерла.

Благодарности

Эта статья представляет собой расширенный и переработанный вариант работы [25]. Здесь подытожена позиция автора, эксплицированная на кулуарных дискуссиях во время Минисимпозиума по выпуклому анализу в Московском государственном университете им. М.В. Ломоносова 2–4 февраля 2007 г. Выражаю свою товарищескую признательность В.М. Тихомирову, председателю минисимпозиума, за терпение, дружелюбие и гостеприимство.

Большую помощь в работе над статьёй автору оказали принципиальная позиция и внимание других учёных и, в первую очередь, прямых учеников А.Н. Колмогорова — В.И. Арнольда, А.А. Боровкова и Я.Г. Синая.

Автор признателен С.П. Новикову за плодотворное обсуждение «дела Лузина» и тонкие комментарии к статье.

Автор получил значительное число откликов и комментариев с критикой, советами по улучшению статьи и указаниями новых документальных источни-

ков и свидетельств. Благодарю всех своих читателей и корреспондентов.

Литература

1. Демидов С.С., Левшин Б.В. (Отв. ред.) Дело академика Николая Николаевича Лузина. Санкт-Петербург : Русский христианский гуманитарный институт, 1999.
2. Lorentz G.G. Mathematics and Politics in the Soviet Union from 1928 to 1953 // Journal of Approximation Theory. 2002. N. 116 P. 169–223.
3. Новиков С.П. История первая: Семья Новиковых–Келдышей и 20 век. URL: `http://www.mi.ras.ru/~snovikov/Mem.pdf` (дата обращения: 20.01.2011).
4. Lorentz G.G., Who Discovered Analytic Sets? // Mathematical Intelligencer. 2001. N. 4(23). P. 28–32.
5. Юшкевич А.П. Мои немногие встречи с А.Н. Колмогоровым. В кн.: Колмогоров в воспоминаниях / Под редакцией А.Н. Ширяева. М. : Физматлит, 1993. С. 602–617.
6. Александров П.С. Страницы автобиографии // Успехи математических наук. 1979. № 4(34). С. 219–249.
7. Лаврентьев М.А. Николай Николаевич Лузин (к 90-летию со дня рождения) // Успехи математических наук. 1974. № 5(29). С. 177–182.
8. Лаврентьев М.А. Наука. Технический прогресс. Кадры. Новосибирск : Наука, 1980.
9. Лаврентьев М.М. Отец не предвидел таких поворотов. В кн.: Городок.ru. Новосибирск : Ин-т перспективных исследований, 2003. С. 45–52.
10. Юшкевич А.П. «Дело» академика Н.Н. Лузина. В кн.: Репрессированная наука. Л. : Наука, 1991. С. 377–394.
11. Тихомиров В.М. Андрей Николаевич Колмогоров. М. : Наука, 2006.
12. Лебег А. Предисловие к книге Н.Н. Лузина «Лекции об аналитических множествах и их приложениях» // Успехи математических наук. 1985. № 3(40). С. 9–14.
13. Дюгак П. «Дело» Лузина и французские математики // Историко-математические исследования. 2000. № 5(40). С. 119–142.
14. Graham L., Kantor J.-M. Naming Infinity: A True Story of Religious Mysticism and Mathematical Creativity. Cambridge and London : The Belknap Press of the Harvard University Press, 2009.
15. Никольский С.М. Мой век. М. : Фазис, 2005.
16. Гордон Е.И. Письма Л.С. Понтрягина И.И. Гордону // Историко-математические исследования. 2005. № 9(44). С. 27–108.
17. Арнольд В.И. Об А.Н. Колмогорове. В кн.: Колмогоров в воспоминаниях учеников. М. : Изд. МЦНМО, 2006. С. 34–53.
18. Вернадский В.И. Дневники. 1935–1941. Книга 1. 1935–1938. М. : Наука, 2006.
19. Антипенко Л.Г. Н.Н. Лузин: Письма к В.И. Вернадскому (Архив АН СССР, Моск. отдел, фонд 518, опись 3, ед. хран. 995) // Русская мысль. 1993. № 1–2. С. 103–117.
20. Боголюбов А.Н., Роженко Н.М. Опыт «внедрения» диалектики в математику в конце 20-х — начале 30-х гг. // Вопросы философии. 1991. № 9. С. 32–43.
21. Понтрягин Л.С. Жизнеописание Льва Семеновича Понтрягина, математика, составленное им самим. Рождения 1908, г. Москва. М. : ИЧП «Прима В», 1998.
22. Решетняк Ю.Г., Кутателадзе С.С. Письмо Н.Н. Лузина Л.В. Канторовичу // Вестник РАН. 2002. № 8(72). С. 740–742.

23. Есаков В.Д. (Сост.) Академия наук в решениях Политбюро ЦК РКП(б)–ВКП(б)–КПСС. 1922–1952. Российская политическая энциклопедия, 2000.
24. Колчинский Э.И. Наука и консолидация советской системы в предвоенные годы В кн.: Наука и кризисы. Историко-сравнительные очерки. Санкт-Петербург : «Дмитрий Булавин», 2003. С. 728–781.
25. Кутателадзе С.С. Корни дела Лузина // Сибирский журнал индустриальной математики. 2007. № 2(10). С. 85–92.

Математические структуры и моделирование
2012, вып. 26, с. 38–48

УДК 517.968

УРАВНЕНИЕ ПЕРВОГО РОДА ОТНОСИТЕЛЬНО МЕРЫ НА СФЕРЕ S^{n-1}

В.Н. Степанов

Исследуются свойства интегрального оператора с ядром, зависящим от скалярного произведения и действующего на банаховом пространстве мер на сфере.

Пусть S^{n-1} — единичная сфера в $\mathbb{R}^n$; u, v — точки на S^{n-1}; $\mathcal{M}$ — банахово пространство знакопеременных мер (зарядов) на S^{n-1} с нормой $\|\mu\| = |\mu|(S^{n-1})$, где $|\mu|(S^{n-1})$ — полная вариация знакопеременной меры μ на S^{n-1}, определяемая формулой [1]

$$\|\mu\| = |\mu|(S^{n-1}) = \sup \left| \int_{S^{n-1}} x(v)\mu(dv) \right|.$$

Здесь sup берётся по всем μ — измеримым функциям $x(v)$ на S^{n-1}, для которых $|x(v)| \leqslant 1$; dv — евклидов элемент площади на S^{n-1}. Норму меры $\|\mu\|$ можно понимать и как наименьшее из чисел $m \geqslant 0$, для которых $\mu(\varphi) \leqslant m \cdot \|\varphi\|$ для любой функции $\varphi(u) \in C(S^{n-1})$. Здесь μ мера Радона на компактном пространстве S^{n-1} [2]. Через $C^a(T)$ обозначено пространство вещественных аналитических функций на компакте $T \subset \mathbb{R}^n$.

Рассмотрим линейное уравнение первого рода

$$(A\mu)(u) \equiv f(u) = \int_{S^{n-1}} K(\langle u, v\rangle)\mu(dv) \tag{1}$$

относительно меры μ на S^{n-1}. $K(\langle u, v\rangle)$ — заданная функция (ядро); $\langle \cdot, \cdot \rangle$ — скалярное произведение.

Интегральные преобразования, определённые формулой (1), тесно связаны с задачами геометрической томографии, которая имеет дело с восстановлением компактного множества B в $\mathbb{R}^n$ по мерам проекций тела на подпространство и по мерам сечений тела подпространствами [3]. Приведём примеры.

1. Сферическое преобразование Радона $(Rf)(u)$:

$$(Rf)(u) = \int_{S^{n-1}} \delta(\langle u, v\rangle) f(v)\mu(dv),$$

Copyright © 2012 **В.Н. Степанов**
Омский государственный технический университет
E-mail: stpnv@yandex.ru

где $\delta(\langle u,v\rangle)$ — дельта-функция и интегрирование выполняется по большой подсфере ортогональной вектору $u \in S^{n-1}$. Если $(n-1)f(v) = \rho^{n-1}$, где ρ радиальная функция звёздного тела B, то $(Rf)(u)$ есть объём пересечения тела B с подпространством $u^{\perp}$ ортогональным вектору $u \in S^{n-1}$.

2. Полусферическое преобразование $(Hf)(u)$:

$$(Hf)(u) = \int_{S^{n-1}} \chi(\langle u,v\rangle)\, f(v)\mu(dv),$$

где $\chi(\langle u,v\rangle)$ — функция Хевисайда. Если функция $f(v)$ равна произведению главных радиусов кривизны гладкой выпуклой поверхности ∂B в точке с нормалью v, то $(Hf)(u)$ представляет площадь «освещённой» части тела B.

3. Косинус преобразование $(Cf)(u)$:

$$(Cf)(u) = \frac{1}{2}\int_{S^{n-1}} |\langle u,v\rangle|\, f(v)\mu(dv).$$

Если функция $f(v)$ равна произведению главных радиусов кривизны гладкой выпуклой поверхности ∂B в точке с нормалью v, то $(Cf)(u)$ равна $(n-1)$-мерному объёму проекции выпуклого тела B на подпространство $u^{\perp}$.

4. p-косинус преобразование $(C_pf)(u)$

$$(C_pf)(u) = \frac{1}{2}\int_{S^{n-1}} |\langle u,v\rangle|^p f(v)\mu(dv).$$

5. Синус преобразование

$$(Sf)(u) = \int_{S^{n-1}} \sqrt{1-\langle u,v\rangle^2} f(v)\mu(dv).$$

О применении этих и других интегральных преобразований вида (1) в геометрической томографии см. [3, 4] и цитированную там литературу.

В работе рассматриваются свойства интегральных операторов вида (1) на пространстве мер.

Теорема 1.

1. *Если* $K(t) \in C[-1,1]$, *то* A — *вполне непрерывный оператор из пространства* $\mathcal{M}$ *в пространство* $C(S^{n-1})$.

2. *Если* $K(t) \in C[-1,1]$, *то* A — *вполне непрерывный оператор из пространства* $\mathcal{M}$ *в пространство* $L_p(S^{n-1};\mu)$, $1 \leqslant p \leqslant \infty$.

3. *Если* $K(t) \in L_p[-1,1], 1 \leqslant p \leqslant \infty$, *то* A — *вполне непрерывный оператор из пространства* $\mathcal{M}$ *в пространство* $L_p(S^{n-1};\mu)$, $1 \leqslant p \leqslant \infty$.

4. *Если* $K(t) \in C^k[-1,1]$, $1 < k < \infty$, *то* A — *вполне непрерывный оператор из пространства* $\mathcal{M}$ *в пространство* $C^k(S^{n-1})$.

5. *Если* $K(t) \in C^{\infty}[-1,1]$, *то* A — *вполне непрерывный оператор из пространства* $\mathcal{M}$ *в пространство* $C^{\infty}(S^{n-1})$.

6. Если $K(t) \in C^a[-1,1]$, то A — вполне непрерывный оператор из пространства $\mathcal{M}$ в пространство $C^a(S^{n-1})$.

Доказательство. $n^0 1$. Пусть $\mathcal{M}' = \{\mu \in \mathcal{M} : \|\mu\| \leqslant m\}$ — ограниченное множество в пространстве $\mathcal{M}$ и множество функций $F = \{f : f = A\mu, \mu \in \mathcal{M}'\}$.

(a_0): множество функций F равномерно ограничено. Действительно, для всех $\mu \in \mathcal{M}'$ выполняется неравенство:

$$|f(u)| = |(A\mu)(u)| \leqslant \int_{S^{n-1}} |K(\langle u, v\rangle)|\,|\mu|(dv) \leqslant \max_{-1\leqslant t\leqslant 1}|K(t)|\,\|\mu\| \leqslant$$
$$\leqslant m \cdot \max_{-1\leqslant t\leqslant 1}|K(t)|$$

для любой функции $f \in F$.

(b_0): множество функций F равностепенно непрерывно. В самом деле, вследствие равномерной непрерывности функции $K(t)$ на отрезке $[-1,1]$ для любого $\varepsilon > 0$ найдётся $\delta = \delta(\varepsilon) > 0$ такое, что для любых $t_1 = \langle u_1, v\rangle$ и $t_2 = \langle u_2, v\rangle$ и любых $v \in S^{n-1}$, как только

$$|t_2 - t_1| = |\langle u_2, v\rangle - \langle u_1, v\rangle| \leqslant |u_2 - u_1| < \delta,$$

сразу же

$$|K(t_2) - K(t_1)| = |K(\langle u_2, v\rangle) - K(\langle u_1, v\rangle)| < \frac{\varepsilon}{m}.$$

Но тогда при $|\langle u_2, v\rangle - \langle u_1, v\rangle| \leqslant |u_2 - u_1| < \delta$ для любой функции $f \in F$ имеем

$$|f(u_2) - f(u_1)| = |(A\mu)(u_2) - (A\mu)(u_1)| \leqslant \int_{S^{n-1}} |K(\langle u_2, v\rangle) - K(\langle u_1, v\rangle)|\,|\mu|(dv) \leqslant$$
$$\leqslant \frac{\varepsilon}{m} \cdot m = \varepsilon,$$

что означает равностепенную непрерывность множества функций F.

Таким образом, множество функций $F = \{f(u) : f(u) = (A\mu)(u),\ \mu \in \mathcal{M}'\}$ равномерно ограничено и равностепенно непрерывно в $C(S^{n-1})$, а поэтому A вполне непрерывный (компактный) оператор из $\mathcal{M}$ в $C(S^{n-1})$. Для нормы оператора A очевидна оценка $\|A\| \leqslant \max\limits_{-1\leqslant t\leqslant 1}|K(t)|$.

$n^0 2$. В $n^0 1$ было доказано, что оператор A с непрерывным ядром является вполне непрерывным оператором из пространства $\mathcal{M}$ в пространство $C(S^{n-1})$.

Пусть $\{\mu_n\}$ — ограниченная последовательность мер из пространства $\mathcal{M}$. Оператор A с непрерывным ядром переводит последовательность $\{\mu_n\}$ в последовательность $\{f_n\} \subset C(S^{n-1})$, $f_n = A\mu_n$. Так как A вполне непрерывный оператор, то из последовательности $\{f_n\}$ можно выбрать подпоследовательность $\{f_k\}$, сходящуюся равномерно к элементу $f_0 \in C(S^{n-1})$. Из вложений $C(S^{n-1}) \subset L_p(S^{n-1}), 1 \leqslant p \leqslant \infty$ следует

$$||f_k - f_0||_{L_p} \leqslant \mathrm{Const}\,||f_k - f_0||_C.$$

Так как при $k \to \infty$, $f_k \rightrightarrows f_0$ равномерно, то $f_k \to f_0$ тем более в $L_p(S^{n-1})$. Это означает, что последовательность $\{f_k\}$ компактна в $L_p(S^{n-1};\mu)$. Следовательно, оператор A — вполне непрерывный оператор из $\mathcal{M}$ в $L_p(S^{n-1};\mu)$ для любого $1 \leqslant p \leqslant \infty$.

$n^0 3$. Отметим для дальнейшего, что интегралы вида

$$\int_{S^{n-1}} K(\langle u,v\rangle)dv, \quad n \geqslant 3$$

не зависят от u и равны [6, с. 214]

$$|S^{n-1}| \int_{-1}^{1} K(t)(1-t^2)^{\frac{n-3}{2}}dt.$$

Пусть $K(t) \in L_p[-1,1], 1 < p < \infty$. Непрерывные функции образуют в пространстве $L_p[-1,1]$ всюду плотное множество. Следовательно, найдётся последовательность $\{K_m(t)\}$ непрерывных на $[-1,1]$ функций, сходящаяся к $K(t)$ в метрике $L_p[-1,1], 1 < p < \infty$, т. е.

$$\int_{-1}^{1} |K_m(t) - K(t)|^p dt \to 0 \quad \text{при} \quad m \to \infty.$$

Но тогда для $n \geqslant 3$ и $1 < p < \infty$

$$\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p du = |S^{n-1}| \int_{-1}^{1} |K_m(t) - K(t)|^p (1-t^2)^{\frac{n-3}{2}} dt \leqslant$$
$$\leqslant |S^{n-1}| \int_{-1}^{1} |K_m(t) - K(t)|^p dt \to 0 \quad \text{при} \quad m \to \infty.$$

Обозначим через A_m интегральные операторы с непрерывными ядрами $K_m(\langle u,v\rangle)$. Применяя неравенство Гёльдера с показателем $1 < p < \infty$, получим:

$$|(A_m\mu)(u) - (A\mu)(u)| = \left| \int_{S^{n-1}} [K_m(\langle u,v\rangle) - K(\langle u,v\rangle)]\mu(dv) \right| \leqslant$$
$$\leqslant \int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)| \cdot 1 \cdot |\mu|(dv) \leqslant$$
$$\leqslant \left[\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p \ |\mu|(dv) \right]^{\frac{1}{p}} \cdot \left[\int_{S^{n-1}} 1^q \ |\mu|(dv) \right]^{\frac{1}{q}} =$$
$$\leqslant \left[\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p \ |\mu|(dv) \right]^{\frac{1}{p}} \cdot ||\mu||^{\frac{1}{q}},$$

где $\frac{1}{p} + \frac{1}{q} = 1, p \neq 1$.

Возводя это неравенство в степень p, интегрируя по мере Лебега du на S^{n-1} и меняя порядок интегрирования, получим:

$$\int_{S^{n-1}} |(A_m\mu)(u) - (A\mu)(u)|^p\, du \leqslant \int_{S^{n-1}} \left[\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p\ |\mu|(dv)\right] du\cdot$$

$$||\mu||^{\frac{p}{q}} = \int_{S^{n-1}} \left[\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p\, du\right] |\mu|(dv)\cdot \|\mu\|^{\frac{p}{q}} =$$

$$= \int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p\, du \cdot \int_{S^{n-1}} |\mu|(dv)\cdot ||\mu||^{\frac{p}{q}} =$$

$$= \int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p\, du \cdot ||\mu||^p,$$

так как $\|\mu\|\cdot\|\mu\|^{\frac{p}{q}} = \|\mu\|^{1+\frac{p}{q}} = \|\mu\|^p$.

Таким образом,

$$||(A_m\mu)(u) - (A\mu)(u)||_{L_p(S^{n-1};\mu)} \leqslant \left(\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p\, du\right)^{\frac{1}{p}}\cdot$$

$$\cdot\, ||\mu|| \leqslant |S^{n-1}|^{\frac{1}{p}} \left(\int_{-1}^{1} |K_m(t) - K(t)|^p\, dt\right)^{\frac{1}{p}} \cdot ||\mu|| \qquad (2)$$

и, следовательно,

$$||A_m - A|| \leqslant \left(\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|^p\, du\right)^{\frac{1}{p}} \to 0 \quad \text{при} \quad m\to\infty,$$

$1 < p < \infty$.

Так как последовательность A_m вполне непрерывных операторов из $\mathcal{M}$ в $L_p(S^{n-1};\mu)$ с непрерывными ядрами равномерно сходится к оператору A с ядром класса $L_p[-1,1], 1 < p < \infty$, то оператор A также вполне непрерывный оператор из пространства $\mathcal{M}$ в пространство $L_p(S^{n-1};\mu)$.

В случае суммируемого ядра, $p = 1$, имеем

$$|(A_m\mu)(u) - (A\mu)(u)| \leqslant \int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|\cdot|\mu|(dv).$$

Интегрируя по u на S^{n-1} и меняя порядок интегрирования, получим:

$$\int_{S^{n-1}} |(A_m\mu)(u) - (A\mu)(u)|du \leqslant \left(\int_{S^{n-1}} |K_m(\langle u,v\rangle) - K(\langle u,v\rangle)|du\right)\cdot||\mu||.$$

Отсюда, как и выше, также следует компактность предельного оператора.

Наконец, пусть $p = \infty$, т. е. ядро $K(t) \in L_\infty[-1,1]$ и $K_m(t)$ последовательность непрерывных ядер, сходящаяся к $K(t)$ в $L_\infty[-1,1]$. Так как для любой функции $\varphi(u) \in L_\infty(S^{n-1};\mu)$

$$||\varphi(u)||_{L_\infty(S^{n-1};\mu)} = \lim_{p\to\infty} ||\varphi(u)||_{L_p(S^{n-1};\mu)},$$

то, переходя в (2) к пределу при $p \to \infty$, получим:

$$||(A_m\mu)(u) - (A\mu)(u)||_{L_\infty(S^{n-1};\mu)} \leqslant ||K_m(t) - K(t)||_{L_\infty[-1,1]} \cdot ||\mu|| \to 0,\ m \to \infty.$$

Следовательно, последовательность операторов A_m сходится равномерно к оператору A. Так как A_m — вполне непрерывные операторы из $\mathcal{M}$ в $L_\infty(S^{n-1};\mu)$, то и в этом случае предельный оператор A — вполне непрерывный как оператор из $\mathcal{M}$ в $L_\infty(S^{n-1};\mu)$.

$n^0 4$. Для доказательства этого утверждения понадобится теорема Титце-Урысона [7, с. 242]: *пусть Q непустой компакт, Q_0 — компактное подмножество Q и $f_0 \in C(Q_0,\mathbb{R})$. Тогда существует функция $f \in C(Q,\mathbb{R})$ такая, что $f|_Q = f_0$.*

Пусть $K(t) \in C^k[-1,1]$, $1 < k < \infty$. По доказанному в $n^0 1$ функция $f(u)$ по крайней мере непрерывна. По теореме Титце-Урысона функцию $f(u)$ можно продолжить в замкнутую область $\overline{Q}_h = \{x \in R^n : 1-h \leqslant |x| \leqslant 1+h, 0 < h < 1\}$.

Для $x \in \overline{Q}_h$ положим:

$$f^*(x) = \int_{S^{n-1}} K\left(\left\langle \frac{x}{|x|}, v\right\rangle\right)\mu(dv).$$

Если $K(t) \in C^k[-1,1]$, где $t = \left\langle \dfrac{x}{|x|}, v\right\rangle$, $1 < k < \infty$, то функция $K\left(\left\langle \dfrac{x}{|x|}, v\right\rangle\right)$ при каждом $v \in S^{n-1}$ имеет непрерывные производные в $\overline{Q}_h$ по x порядка α, $|\alpha| \leqslant k$, равные

$$D_x^\alpha K\left(\left\langle \frac{x}{|x|}, v\right\rangle\right) = \sum_{i=1}^{|\alpha|} d_i \cdot K^{(|\alpha|+1-i)}(t),$$

где коэффициенты d_i содержат производные от $t = \left\langle \dfrac{x}{|x|}, v\right\rangle$ порядка не выше i.

Следовательно, по теореме о дифференцируемости функции, представимой интегралом, функция $f^*(x) \in C^k(\overline{Q}_h)$ и

$$D^\alpha f^*(x) = \int_{S^{n-1}} D_x^\alpha K\left(\left\langle \frac{x}{|x|}, v\right\rangle\right)\mu(dv), \quad |\alpha| \leqslant k.$$

Значит $f(u) \in C^k(S^{n-1})$ и

$$D^\alpha f(u) \equiv D^\alpha f^*(x)|_{x=u} = \int_{S^{n-1}} D_x^\alpha\ K\left(\left\langle \frac{x}{|x|}, v\right\rangle\right)\Big|_{x=u}\mu(dv) = \tag{3}$$

$$= \sum_{i=1}^{|\alpha|}\int_{S^{n-1}} d_i \cdot K^{(|\alpha|+1-i)}(t)\big|_{x=u}\,\mu(dv).$$

Так как для производных $D^\alpha f(u)$ (которые определены равенством $D^\alpha f(u) = D^\alpha f^*(x)|_{x=u}$) имеет место оценка:

$$|D^\alpha f(u)| \leqslant c_\alpha ||K(t)||_{C^{|\alpha|}[-1,1]} \cdot ||\mu||, \quad |\alpha| \leqslant k,$$

то

$$||f(u)|\,|_{C^k(S^{n-1})} \leqslant C \cdot ||\mu||$$

при $1 < k < \infty$. Постоянная C зависит от k и $||K(t)||_{C^k[-1,1]}$. Следовательно, оператор $A : \mathcal{M} \to C^k(S^{n-1})$ непрерывен.

Для доказательства полной непрерывности оператора A воспользуемся следующим критерием компактности в пространстве $C^k(\overline{G})$, идея доказательства которого содержится в известной теореме Арцела-Асколи.

Критерий компактности в пространстве $C^k(\overline{G})$. *Пусть G — связное ограниченное множество в $\mathbb{R}^n$. Для того чтобы множество функций $\Phi \subset C^k(\overline{G})$ было компактно в $C^k(\overline{G})$ необходимо и достаточно, чтобы*
(a_k): множество Φ было ограничено, т. е.

$$|f(x)| \leqslant M, \ \ \forall x \in \overline{G}, \ \forall f \in \Phi;$$

(b_k): производные функций из множества Φ были равностепенно непрерывны: $\forall \varepsilon > 0 \ \exists \ \delta > 0$ такое, что $\forall \ x, y \in \overline{G}$ из $|x - y| < \delta$ следует

$$|D^\alpha f(x) - D^\alpha f(y)| < \varepsilon, \ \ \forall \alpha, \ |\alpha| = k, \ \forall f \in \Phi.$$

Пусть

$$(A\mu)(u) \equiv f(u) = \int_{S^{n-1}} K(\langle u, v\rangle)\mu(dv)$$

и ядро $K(t) \in C^k[-1, 1]$, $1 < k < \infty$. Выше доказано, что функция $f(u) \in C^k(S^{n-1})$, следовательно, оператор A действует из пространства $\mathcal{M}$ в пространство $C^k(S^{n-1})$ и является непрерывным оператором. Для доказательства полной непрерывности оператора A проверим выполнение условий (a_k) и (b_k).

Пусть $\mathcal{M}' = \{\mu \in \mathcal{M} : ||\mu|| \leqslant m\}$ — ограниченное множество в пространстве мер $\mathcal{M}$ и множество функций $F = \{f : f = A\mu, \ \mu \in \mathcal{M}'\}$.

(a_k). Множество функций F равномерно ограничено. Действительно, для всех $\mu \in \mathcal{M}'$ выполняется неравенство:

$$|(A\mu)(u)| \leqslant \int_{S^{n-1}} |K(\langle u, v\rangle)||\mu|(dv) \leqslant \max_{-1\leqslant t\leqslant 1}|K(t)|\,\|\mu\| \leqslant m \cdot \max_{-1\leqslant t\leqslant 1}|K(t)|$$

для любой функции $f \in F$.

(b_k). Производные от функций из множества F порядков $|\alpha| \leqslant k$ равностепенно непрерывны. Действительно, вследствие равномерной непрерывности производных $D^\alpha K(\langle u, v\rangle)$ на S^{n-1} для любого $\varepsilon > 0$ найдётся такое $\delta = \delta(\varepsilon)$, что для любых u_1, $u_2 \in S^{n-1}$ и для любого $v \in S^{n-1}$ из неравенства $|u_2 - u_1| < \delta$ следует неравенство:

$$|D^\alpha K(\langle u_2, v\rangle) - D^\alpha K(\langle u_1, v\rangle)| < \varepsilon.$$

Используя равенство (3), для любой функции $f \in F$ имеем:

$$|D^\alpha f(u_2) - D^\alpha f(u_1)| \leqslant \int_{S^{n-1}} |D^\alpha K(\langle u_2, v\rangle) - D^\alpha K(\langle u_1, v\rangle)| \cdot |\mu|(dv) \leqslant$$

$$\leqslant \varepsilon \cdot m,$$

что означает равностепенную непрерывность производных порядков $|\alpha| \leqslant k$ функций из множества F. По критерию компактности множество F компактно и оператор $A : \mathcal{M} \to C^k(S^{n-1})$ вполне непрерывен.

$n^0 5$. Прежде всего отметим, что оператор A с ядром $K(\langle u, v\rangle)$ класса $C^\infty[-1,1]$ действует из пространства $\mathcal{M}$ в пространство $C^\infty(S^{n-1})$. Это следует из доказательства в $n^0 1$ и $n^0 4$, где показано, что для любого α, $|\alpha| \geqslant 0$

$$D^\alpha f(u) = D^\alpha f^*(x)|_{x=u} = \int_{S^{n-1}} D_x^\alpha \, K\left(\left\langle \frac{x}{|x|}, v \right\rangle\right)\Big|_{x=u} \mu(dv) = \tag{4}$$
$$= \int_{S^{n-1}} D_u^\alpha K\left(\langle u, v\rangle\right) \mu(dv).$$

Поэтому, если ядро класса $C^\infty[-1,1]$, то и функция $f(u) \in C^\infty(S^{n-1})$.

В пространстве $C^\infty(S^{n-1})$ бесконечное число раз дифференцируемых на S^{n-1} функций определим разделяющее семейство $\mathcal{P}$ согласованных полунорм $p_m(f)$, $m = 0, 1, 2, \ldots$, полагая

$$p_m(f) = \max_{u \in S^{n-1},\, |\alpha| \leqslant m} \left| D^\alpha f(u) \right|.$$

Обычным способом в $C^\infty(S^{n-1})$ введём топологию, принимая за локальную базу окрестностей нуля, например, множества

$$U_m = \left\{ f \in S^{n-1} : p_m(f) < \frac{1}{m+1},\, m = 0, 1, 2, \ldots \right\}.$$

Так как $\mathcal{P} = \{p_m(f)\}_{m=0}^\infty$ счётное разделяющее семейство согласованных полунорм, то пространство $C^\infty(S^{n-1})$ является локально выпуклым счётно-нормированным пространством [1, с. 45], [8, с. 33]. Как известно, [8, с. 25], [14, с. 103], топологическое векторное пространство со счётной локальной базой метризуемо. Инвариантная относительно сдвигов метрика, совместимая с введённой топологией, может быть определена формулой

$$\rho(f, g) = \sum_{m=0}^{\infty} \frac{1}{2^m} \cdot \frac{p_m(f-g)}{1 + p_m(f-g)}. \tag{5}$$

Пространство $(C^\infty(S^{n-1}); \rho)$ — полное [9, с. 16] локально выпуклое метрическое пространство, т. е. является пространством Фреше. Как показано в [8, с. 44], это пространство обладает свойством Гейне-Бореля: в нём любое ограниченное замкнутое множество компактно.

Поэтому для доказательства полной непрерывности оператора A достаточно установить, что множество

$$F = \left\{ f \in C^\infty(S^{n-1}) : f(u) = (A\mu)(u), ||\mu|| \leqslant m \right\}$$

замкнуто и ограничено в $(C^\infty(S^{n-1}); \rho)$.

Ограниченность множества F в локально выпуклом пространстве равносильна ограниченности каждой полунормы на F [8, с. 35]. Оценка $p_n(f) \leqslant c_n$, $n = 0, 1, 2, \ldots$ следует из равенства (4).

Докажем замкнутость множества F. Пусть $f_0(u)$ — предельная точка (функция) множества F. Тогда существует последовательность $\{f_n(u)\} \subset F$, сходящаяся к $f_0(u)$ в метрике пространства $C^\infty(S^{n-1})$ и, следовательно, функция $f_0(u) \in C^\infty(S^{n-1})$, ввиду полноты $C^\infty(S^{n-1})$. Так как $f_n(u) \in F$ при каждом n, то по определению множества F существует ограниченная мера μ_n, $\|\mu_n\| \leqslant m$, такая что $f_n(u) = (A\mu_n)(u)$. По теореме Банаха-Алаоглу [10, с. 459], [2, с. 75] из ограниченной последовательности мер $\{\mu_n\}$ можно выбрать слабо сходящуюся подпоследовательность $\{\mu_k\}$. Пусть $\mu_k \underset{\text{слабо}}{\rightharpoonup} \mu_0$, т. е. $\mu_k(\varphi) \to \mu_0(\varphi)$ для любой функции $\varphi(u) \in C^\infty(S^{n-1})$, где значение меры μ на функции $\varphi(u) \in C^\infty(S^{n-1})$ понимается как интеграл по S^{n-1} от $\varphi(u)$ по мере μ [2, с. 63] и пусть $f_k(u) = (A\mu_k)(u)$. Последовательность мер μ_k слабо сходится к мере μ_0, поэтому для любого $u \in S^{n-1}$

$$\lim_{k\to\infty} \int_{S^{n-1}} K(\langle u, v\rangle)\mu_k(dv) = \int_{S^{n-1}} K(\langle u, v\rangle)\mu_0(dv) = \widehat{f_0}(u).$$

Так как ядро $K(\langle u, v\rangle)$ класса $C^\infty[-1, 1]$, то и функция $\widehat{f_0}(u)$ бесконечное число раз дифференцируема на S^{n-1}.

Покажем теперь, что если $\mu_k \underset{\text{слабо}}{\rightharpoonup} \mu_0$ и последовательность мер $\{\mu_k\}$ ограничена, $\|\mu_n\| \leqslant m$, то мера μ_0 также ограничена, $\|\mu_0\| \leqslant m$. Как отмечалось, норму меры на компактном пространстве можно определить следующим образом: $\|\mu\| = \{\inf c : |\mu(\varphi)| \leqslant c, \forall\varphi \in C(S^{n-1})\}$ [2, с. 60].

Так как $\mu_0(\varphi) = \lim_{k\to\infty} \mu_k(\varphi)$ для любой функции $\varphi(u) \in C^\infty(S^{n-1})$, то $|\mu_0(\varphi)| = \lim_{k\to\infty} |\mu_k(\varphi)|$. Для последовательности $\{\mu_k(\varphi)\}$ имеем оценку $|\mu_k(\varphi)| \leqslant \|\mu_k\| \cdot \|\varphi\|$. По условию числовая последовательность $\{\|\mu_k\|\}$ ограничена, $\|\mu_k\| \leqslant m$, поэтому существует её верхний предел $\overline{\lim}_{k\to\infty}\|\mu_k\| \leqslant m$. Следовательно,

$$|\mu_0(\varphi)| = \lim_{k\to\infty} |\mu_k(\varphi)| \leqslant \overline{\lim}_{k\to\infty}\|\mu_k\| \cdot \|\varphi\| \leqslant m\|\varphi\|, \ \ \forall\varphi \in C(S^{n-1}).$$

Отсюда получаем оценку $\|\mu_0\| \leqslant m$, поэтому функция $\widehat{f_0}(u) \in F$.

Так как последовательность функций $\{f_n(u)\}$ сходится к функции $f_0(u)$ в метрике пространства $C^\infty(S^{n-1})$, то и её подпоследовательность $\{f_k(u)\}$ также сходится к функции $f_0(u)$ в метрике пространства $C^\infty(S^{n-1})$. Значит $\widehat{f_0}(u) = f_0(u)$. Таким образом, предельная функция $f_0(u) \in F$, множество F замкнуто и оператор $A : \mathcal{M} \to C^\infty(S^{n-1})$ вполне непрерывен.

$n^0 6$. Пусть ядро $K(\langle u, v\rangle)$ оператора A — аналитическая на отрезке $[-1, 1]$ функция. В работах [11, 12] показано, что интегральный оператор A с аналитическим ядром действует из пространства $\mathcal{M}$ в пространство $C^a(S^{n-1})$.

В пространстве $C^a(S^{n-1})$ аналитических на S^{n-1} функций определим семейство $\mathcal{P}$ полунорм $p_m(f), m = 0, 1, 2, \ldots$, локальную базу $\{U_m\}$ окрестностей

нуля и инвариантную относительно сдвигов метрику ρ так же, как и в предыдущем пункте по формуле (5). Тогда пространство $(C^a(S^{n-1});\rho)$ будет локально выпуклым счётно-нормированным метрическим пространством. Установим полноту этого пространства.

Пусть $\{f_n(u)\}$ фундаментальная относительно метрики ρ последовательность, т. е. $\{f_n(u)\} \subset C^a(S^{n-1})$ и $\rho(f_i, f_j) \to 0$ при $i, j \to \infty$. Так как сходимость по метрике ρ есть «покоординатная» сходимость, то фундаментальная по метрике ρ последовательность будет фундаментальной по любой полунорме, поэтому $p_m(f_i - f_j) = \max_{u\in S^{n-1},|\alpha|\leqslant m} |D^\alpha f_i(u) - D^\alpha f_j(u)| \to 0$. Следовательно, последовательность $\{D^\alpha f_i(u)\}$ сходится равномерно на S^{n-1} при любом фиксированном α, $|\alpha| \geqslant 0$ к некоторой непрерывной функции $f_\alpha(u)$. В частности, $f_i(u) \Rightarrow f_0(u)$; $f_\alpha(u) = D^\alpha f_0(u)$, и поэтому $f_0(u) \in C^\infty(S^{n-1})$. Теперь следует показать, что функция f_0, которая является пределом равномерно сходящейся в метрике ρ последовательности $\{f_n(u)\}$ аналитических на компакте S^{n-1} функций, также является аналитической на S^{n-1} функцией. Это следует из теоремы Вейерштрасса для голоморфных функций нескольких комплексных переменных [9, с. 13]; [13, с. 289]: *если последовательность $\{f_i\}$ голоморфных (аналитических) в области $U \subset C^n$ функций сходится равномерно на компактных подмножествах U к некоторой функции f, то функция f голоморфна в U и для любого α последовательность $D^\alpha f_i$ сходится равномерно к $D^\alpha f$ на компактах из U.*

Пространство $(C^a(S^{n-1});\rho)$ — локально выпукло, и его топология порождается полной инвариантной относительно сдвигов метрикой ρ. Следовательно, оно является пространством Фреше [8].

Следуя [8, с. 44], покажем, что пространство Фреше $(C^a(S^{n-1});\rho)$ обладает свойством Гейне-Бореля: в нём ограниченное замкнутое множество компактно. Пусть $E \subset C^a(S^{n-1})$ — замкнутое ограниченное множество. Ограниченность означает, что каждая полунорма $p_m(f)$ ограничена на E. Пусть $p_m(f) \leqslant c_m < \infty$, $m = 0, 1, 2, \ldots$, для всех $f \in E \subset C^a(S^{n-1})$. Из неравенств $|D^\alpha f(u)| \leqslant c_m$, справедливых на S^{n-1} при $|\alpha| \leqslant m$, следует, что для любого мультииндекса β с $|\beta| \leqslant m-1$, $m = 1, 2, \ldots$, семейство функций $\left\{D^\beta f(u) : f \in E\right\}$ равностепенно непрерывно на S^{n-1}. Применив теорему Арцела-Асколи к семейству функций $\left\{D^\beta f(u) : f \in E\right\}$ при каждом фиксированном β, а затем канторовскую диагональную процедуру, получим, что любая последовательность функций из E содержит такую подпоследовательность f_i, что для любого β последовательность $\{D^\beta f_i\}$ сходится равномерно на S^{n-1}. Следовательно, последовательность $\{f_i\}$ сходится в метрике пространства $C^a(S^{n-1})$, т е. предельная функция аналитическая как предел равномерно сходящейся в метрике ρ на компакте S^{n-1} последовательности аналитических функций. А так как по предположению множество E замкнуто, то предельная функция принадлежит множеству E. Это означает, что E компактное множество. Следовательно, пространство $(C^a(S^{n-1});\rho)$ действительно обладает свойством Гейне-Бореля.

Так как пространство $C^a(S^{n-1})$ обладает свойством Гейне-Бореля и не является локально ограниченным (иначе оно было бы конечномерным [8], стр. 25),

то как следствие получаем, что в пространстве $C^a(S^{n-1})$ не существует нормы, совместимой с введённой топологией.

Остаётся доказать полную непрерывность оператора A. Так как пространство $(C^a(S^{n-1});\rho)$ является пространством Фреше и обладает свойством Гейне-Бореля, то для доказательства полной непрерывности оператора A, как и в предыдущем пункте, достаточно установить, что множество

$$F = \left\{ f \in C^a(S^{n-1}) : f(u) = (A\mu)(u),\ ||\mu|| \leqslant m \right\}$$

замкнуто и ограничено в $(C^a(S^{n-1});\rho)$. Ограниченность полунорм $p_m(f) \leqslant c_m$, $m = 0, 1, 2, \ldots$ также следует из равенства (4). Замкнутость множества F доказывается совершенно аналогично случаю пространства $C^\infty(S^{n-1})$. Следует только иметь в виду, что функция $\widehat{f_0}(u) \in C^a(S^{n-1})$, поскольку ядро $K(\langle u, v\rangle)$ интегрального оператора является аналитической функцией и предельная функция $f_0(u)$ принадлежит пространству $C^a(S^{n-1})$ ввиду его полноты. ■

Литература

1. Иосида К. Функциональный анализ. М. : Наука, 1967. 624 с.
2. Бурбаки Н. Интегрирование. М. : Наука, 1967. 396 с.
3. Gardner R.J. Geometric tomography. New York : Cambridge Univ. Press. Cambridge, 1995. 424 p.
4. Schneider R. Convex bodies: The Brunn-Minkowski Theory. New York : Cambridge Univ. Press. Cambridge, 1993. 490 p.
5. Эдвардс Р. Функциональный анализ. М. : Наука, 1969. 1072 с.
6. Наттерер Ф. Математические аспекты компьютерной томографии. М. : Мир, 1990. 280 с.
7. Кутателадзе С.С. Основы функционального анализа. Новосибирск : Институт математики, 2001. 354 с.
8. Рудин У. Функциональный анализ. М. : Мир, 1975. 446 с.
9. Нарасимхан Р. Анализ на действительных и комплексных многообразиях. М. : Мир, 1971. 32 с.
10. Данфорт Н., Шварц Дж.Т. Линейные операторы. М. : ИЛ, 1962. 896 с.
11. Stepanov V.N. Firs-kind equations on a sphere and some problems of convex geometry // J. Inv. Ill-Posed Problems. 2002. Vol. 20, N. 9, P. 1–20.
12. Степанов В.Н. Асимптотика собственных значений уравнения первого рода // Омский научный вестник. 2011. № 3(103). С. 41–44.
13. Шабат Б.В. Введение в комплексный анализ. М. : Наука, 1969. 576 с.
14. Канторович Л.В. Функциональный анализ. М. : Наука, 1977. 744 с.

Mathematical
Structures and Modeling
2012, N. 26, pp. 49–56

UDC 530.16:51-73

TOWARDS UNIQUE PHYSICALLY MEANINGFUL DEFINITIONS OF RANDOM AND TYPICAL OBJECTS

L. Longpré, O. Kosheleva

To distinguish between random and non-random sequence, Kolmogorov and Martin-Löf proposed a new definition of randomness, according to which an object (e.g., a sequence of 0s and 1s) is random if it satisfies all probability laws, i.e., in more precise terms, if it does not belong to any definable set of probability measure 0. This definition reflect the usual physicists' idea that events with probability 0 cannot happen. Physicists – especially in statistical physics – often claim a stronger statement: that events with a very small probability cannot happen either. A modification of Kolmogorov-Martin-Löf's (KLM) definition has been proposed to capture this physicists' claim. The problem is that, in contrast to the original KLM definition, the resulting definition of randomness is not uniquely determined by the probability measure: for the same probability measure, we can have several different definitions of randomness. In this paper, we show that while it is not possible to define, e.g., a unique *set* $\mathcal{R}$ of random objects, we can define a unique *sequence* $\mathcal{R}_n$ of such sets (unique in some reasonable sense).

1. Definitions of Random and Typical Objects: Reminder

Some sequences are random, some are not. Traditional probability theory does not allow us to distinguish between random and non-random numbers, sequences, etc., it only allows us to determine the probability that, e.g., a random sequence of 0s and 1s – corresponding to flipping a fair coin – belongs to a given set of sequences. However, from the physical viewpoint, some sequences of 0s and 1s are random – in the sense that they can appear as a result of the actual coin tosses – while other cannot. For example, it is intuitively clear that a periodic sequence 0101... cannot result from the actual coin tosses.

Kolmogorov-Martin-Löf randomness. To formalize the above intuitive notion, A. N. Kolmogorov and P. Martin-Löf proposed the following idea. How do we know that a sequence is not random? For example, a sequence 00... (consisting of all 0s) is not random because we know that:

Copyright © 2012 **L. Longpré, O. Kosheleva**
University of Texas at El Paso (USA)
E-mail: longpre@utep.edu, olgak@utep.edu

- for almost all sequence, the proportion of 0s among the first n symbols tends to $1/2$ as $n \to \infty$, while
- for the sequence $00\ldots$, the proportion of 0s is equal to 1.

Similarly, a periodic sequence $0101\ldots$ is not random because:

- for almost all sequence, the frequency of 11 tends to $1/4$, while
- for the periodic sequence $0101\ldots$, this frequency is 0.

Frequency limit is a simple case, we may have more complex reasons why a given sequence is not random.

In general, it is reasonable to say that a sequence is random if it satisfies all the *probability laws*, i.e., all the statements (defined in a certain language L) which are true for almost all sequences. To be more precise, a probability law on the set X of all sequences is an L-definable subset $S \subseteq X$ for which $P(S) = 1$ – or, equivalently, for whose (similarly definable) complement $-S$, we have $P(-S) = 0$. So, we arrive at the following definition.

Definition 1. We say that an object $x \in X$ is *random* in the sense of Kolmogorov-Martin-Löf if it does not belong to any L-definable set of probability 0.

Remark 1. Definable simply means that there is a formula in the corresponding language that uniquely determines the object. For example, in the usual theory of real numbers, 1, 2, π, $\sqrt{2}$, e, any number that can we think of is definable. This does not means, of course, that every real number if definable: in each language L, there are no more countably many words, so there are no more than countably many L-definable real numbers. Thus, there are continuum many real numbers which are not definable.

The notion of an L-definable object cannot be formally described within the language L itself. The proof of this impossibility is a simple modification of the known Berry paradox [1]: if we could describe definability within L, we could, in particular, define the smallest integer that cannot be described by fewer than 100 words. By definition, this integer cannot be described by fewer than 100 words, but the above description "the smallest integer that cannot be described by fewer than 100 words" is a description of this integer in fewer than 100 words – a contradiction.

Thus, to formally talk about L-definability, we need to use a stronger language L_1 in which L-definability can be formally described. For each language L, the existence of such a stronger language L_1 can be easily proven; see, e.g., [2].

Almost all sequences are Kolmogorov-Martin-Löf random. As we have just mentioned, in each language L, there are no more countably many words, so there are no more than countably many L-definable sets of probability 0. Hence, to describe all sequence which are Kolmogorov-Martin-Löf random, we delete, from

the original set X of probability measure 1, a union of countably many L-definable sets of measure 0. A union of countably many set of measure 0 is also of measure 0, so almost all sequences are random in this sense.

Towards a more physically adequate notion of randomness. Kolmogorov-Martin-Löf definition prevents sequences 00... from being called random. This prevention makes perfect physical sense: if we flip a coin and every time get tail, this clearly is not a fair coin.

However, one can easily check that for each random sequence ω, a sequence 0...0 (1,000,000 times) followed by ω is also random in the sense of Kolmogorov-Martin-Löf. This is not physically meaningful: it is clearly not realistically possible to toss a fair coin million times and get tail every time. Physicists usually argue that this situation is not physical because its probability is too low – in the above example, this probability is equal to $2^{-1,000,000}$. This argument is behind the usual applications of statistical physics: e.g., from the purely mathematical viewpoint, it is possible that all the randomly moving molecules of a human body will start going into the same vertical direction, and the person will float on air – but the probability of this event is so small, then it is not physically possible.

This idea cannot be described by simply setting a small threshold $p_0 \ll 1$ and claiming that no event with a probability $\le p_0$ is possible: indeed, for a sequence of n coin tosses, every sequence of 0s and 1s has the same probability 2^{-n}; so, for a sufficiently large n, for which $2^{-n} \le p_0$, we would arrive at a conclusion that no such sequence is possible at all. In other words, the threshold p_0 is not a universal constant, it depends on the property.

In particular, if we are looking for the impossibility to have too many 0s at the beginning, then we have a sequence of sets

$$A_n = \{\omega \text{ starts with } n \text{ zeroes}\} = \{\omega : \omega_1 = \ldots = \omega_n = 0\}$$

for which $A_1 \supseteq A_2 \supseteq \ldots \supseteq A_n \supseteq \ldots$ and $P(A_n) \to 0$ as $n \to \infty$. In general, we have a definable sequence of sets A_n for which $A_n \supseteq A_{n+1}$ and $P(A_n) \to 0$. Our claim is that for each such sequence, there is an N for which $P(A_N)$ is so small that a truly random sequence cannot belong to the set A_N. In other words, we arrive at the following definition of the class $\mathcal{R}$ of random sequences:

Definition 2. We say that a non-empty set $\mathcal{R} \subseteq X$ is *a set of random objects* if for every definable sequence A_n for which $A_n \supseteq A_{n+1}$ and $P(A_n) \to 0$, there exists an N for which $A_N \cap \mathcal{R} = \emptyset$.

Discussion. The existence of such a set follows if we consider a language in which L-definability can be explicitly described; see, e.g., [2]. It turns out that, in contrast to the Kolmogorov-Martin-Löf definition, we cannot have a set of random elements $\mathcal{R}$ for which $P(\mathcal{R}) = 1$. However, we can have a set of random elements which is "almost" of measure 1 [2]. To formulate this result, let us recall that in the continuous case, not every set is measurable, but for every set S, we can define:

- an *inner measure* $\underline{P}(S)$, defined as the supremum of all the values $P(S')$ for all measurable sets $S' \subseteq S$, and
- an *outer measure* $\overline{P}(S)$, defined as the infimum of all the values $P(S')$ for all measurable sets $S' \supseteq S$.

The existence result is that for every $\varepsilon > 0$, we can have a set of random elements $\mathcal{R}$ for which $\underline{P}(\mathcal{R}) \geq 1 - \varepsilon$.

From random to typical. In the above examples, we assume that we know the probability distribution on the set of all possible objects. In some cases, physicists talk about "typical" objects even when no such probability distribution is known. For example, they argue that since "almost all" cosmological solutions of General Relativity theory have a certain asymptotic behavior, the actual University must exhibit the same behavior; see, e.g., [3]. The possibility of such conclusions comes from the fact that if $A_n \supseteq A_{n+1}$ and $\cap A_n = \emptyset$, then $P(A_n) \to 0$ no matter what the probability distribution P is. Thus, we arrive at the following definition:

Definition 3. We say that a non-empty set $\mathcal{T} \subseteq X$ is *a set of typical objects* if for every definable sequence A_n for which $A_n \supseteq A_{n+1}$ and $\cap A_n = \emptyset$, there exists an N for which $A_N \cap \mathcal{T} = \emptyset$.

2. Formulation of the Problem

In contrast to the Kolmogorov-Martin-Löf definition, the new notions are not uniquely determined. The problem dealt with in this paper comes from the fact that the above physically adequate notions of random and typical objects are not uniquely determined.

Indeed, in the Kolmogorov-Martin-Löf's definition, once we know the probability measure P and fix the language L, we can tell which objects are random and which are not. In contrast, we may have several different sets $\mathcal{R}$ and $\mathcal{T}$ that satisfy Definitions 2 and 3.

Let us show that this non-uniqueness is inevitable. Indeed, let us consider a simple situation when we have a uniform probability distribution P on a unit disc

$$D = \{(x, y) : x^2 + y^2 \leq 1\}.$$

This probability distribution is invariant w.r.t. arbitrary rotations around the disk's center $(0, 0)$. So, any definable rotation preserves the situation. Thus, if we had a meaningful way to select a unique set $\mathcal{R}$, this selection would not change under such rotations. It turns out that such an invariance is not possible:

Proposition 1. *Let X be a unit disc D with a uniform distribution P, and let $\mathcal{P} \subseteq X$ be a set of random objects. Then, there exists a definable rotation under which the set $\mathcal{P}$ is not invariant.*

Remark 2. For readers' convenience, all the proofs are placed in the special (last) Proofs section.

Possible reason for non-uniqueness. A possible reason for non-uniqueness is that, as we have mentioned earlier,

- while we cannot have a set of random elements $\mathcal{R}$ with $P(\mathcal{R}) = 1$,
- for every $\varepsilon > 0$, we can have a set of random elements $\mathcal{R}$ for which $\underline{P}(\mathcal{R}) \geq 1 - \varepsilon$.

Thus, to capture the general intuitive meaning of randomness, it is not enough to have *one* set of random elements, it is more appropriate to have a *sequence* of such sets – corresponding to decreasing values of ε.

This is what we will do in this paper.

3. Definitions and the Main Result

Comment about languages. As we have mentioned, we start with a language L in which we describe definable objects. Then, we need a (stronger) language L_1 in which we can formally describe L-definability. It is possible to define L_1-definable sets of random elements and sets of typical elements [2]. We want to formally discuss L_1-definable sets, so we need to introduce yet stronger language L_2 in which such discussions are formally possible. This language can be built from L_1 in the same manner as the language L_1 is built from L.

Definition 4. By a *description of randomness*, we mean a sequence of L_1-definable sets of random elements $\mathcal{R}_n$ for which $\mathcal{R}_n \subseteq \mathcal{R}_{n+1}$.

Definition 5. By a *description of typicality*, we mean a sequence of L_1-definable sets of typical elements $\mathcal{T}_n$ for which $\mathcal{T}_n \subseteq \mathcal{T}_{n+1}$.

When is a description universal? When are two descriptions equivalent? To answer these questions, we can take into account that every non-empty subset of a set of random elements is also a set of random elements, and that every non-empty subset of the set of all typical elements is also a set of typical elements:

Lemma 1. *If $\mathcal{R}$ is a set of random elements, and $\mathcal{S}$ is a non-empty subset of $\mathcal{R}$, then $\mathcal{S}$ is also a set of random elements.*

Lemma 2. *If $\mathcal{T}$ is a set of typical elements, and $\mathcal{S}$ is a non-empty subset of $\mathcal{T}$, then $\mathcal{S}$ is also a set of typical elements.*

Remark 3. The proofs follow directly from Definitions 2 and 3. Now, we can formally describe universality and equivalence.

Definition 6. We say that a description of randomness $\mathcal{R}_n$ is *universal* if for every L_1-definable set of random elements $\mathcal{R}$, there exists n for which $\mathcal{R} \subseteq \mathcal{R}_n$.

Definition 7. We say that a description of typicality $\mathcal{T}_n$ is *universal* if for every L_1-definable set of typical elements $\mathcal{T}$, there exists n for which $\mathcal{T} \subseteq \mathcal{T}_n$.

Definition 8. We say that two descriptions of randomness $\mathcal{R}_n$ and $\mathcal{R}'_n$ are *equivalent* if the following two conditions hold:

- for every natural number n, there exists n' for which $\mathcal{R}_n \subseteq \mathcal{R}'_{n'}$; and
- for every natural number n', there exists n for which $\mathcal{R}'_{n'} \subseteq \mathcal{R}_n$.

Definition 9. We say that two descriptions of typicality $\mathcal{T}_n$ and $\mathcal{T}'_n$ are *equivalent* if the following two conditions hold:

- for every natural number n, there exists n' for which $\mathcal{T}_n \subseteq \mathcal{T}'_{n'}$; and
- for every natural number n', there exists n for which $\mathcal{T}'_{n'} \subseteq \mathcal{T}_n$.

Proposition 2. *There exists a universal description of randomness, and this description is unique modulo equivalence.*

Proposition 3. *There exists a universal description of typicality, and this description is unique modulo equivalence.*

Remark 4. In other words:

- there exists a universal description of randomness, and all universal descriptions of randomness are equivalent to each other, and
- there exists a universal description of typicality, and all universal descriptions of typicality are equivalent to each other.

The proof of Propositions 2 and 3 is based on the following lemmas:

Lemma 3. *For every set X, if $\mathcal{R}'$ and $\mathcal{R}''$ are sets of random elements, then their union $\mathcal{R} \stackrel{\text{def}}{=} \mathcal{R}' \cup \mathcal{R}''$ is also a set of random elements.*

Lemma 4. *For every set X, if $\mathcal{T}'$ and $\mathcal{T}''$ are sets of typical elements, then their union $\mathcal{T} \stackrel{\text{def}}{=} \mathcal{T}' \cup \mathcal{T}''$ is also a set of typical elements.*

4. Proofs

Proof of Proposition 1. Let $\mathcal{P} \subseteq D$ be a set of random objects. Every point $d \in D$ can be described by its polar coordinates (r, θ), where $0 \le r \le 1$ is the distance from this point to $(0, 0)$, and $\theta \in [0, 2\pi)$ is the angle between the direction $0d$ from 0 to this point d and the x-axis. Let us consider the following sequence of sets A_n:

$$A_n = \{(r, \theta) : |\theta| \le 2^{-n}\}.$$

Then, clearly, $A_n \supseteq A_{n+1}$ and $\cap A_n = \emptyset$, so $P(A_n) \to 0$. Thus, by definition of the set of random objects, there exists an integer N for which $A_N \cap \mathcal{P} = \emptyset$. In other words, no point $(r, \theta) \in \mathcal{P}$ can have a value $|\theta| \le 2^{-N}$.

Let us now prove, by contradiction, that the set $\mathcal{P}$ cannot be invariant relative to all possible definable rotations. Indeed, if the set $\mathcal{P}$ was invariant with respect

to arbitrary definable rotations, then it would be invariant with respect to rotation by 2^{-N} radians, by $2 \cdot 2^{-N}$ radians, etc. Since no points with $|\theta| \le 2^{-N}$ are in the set $\mathcal{P}$, by rotating by 2^{-N}, we conclude that no points with $\theta \in [0, 2 \cdot 2^{-N}]$ can be in this set, then that no points with $\theta \in [2^{-N}, 3 \cdot 2^{-N}]$ can be in this set – etc., until we conclude that no points with any value θ are possible and thus, that $\mathcal{P}$ is an empty set. The proposition is proven.

Proof of Lemma 3. To prove that the union $\mathcal{R} = \mathcal{R}' \cup \mathcal{R}''$ is a set of random elements, let us assume that A_n be a definable sequence of sets for which $A_n \supseteq A_{n+1}$ and $P(A_n) \to 0$. We need to prove that there exists an integer N for which $A_N \cap \mathcal{R} = \emptyset$.

Indeed, since $\mathcal{R}'$ is a set of random elements, there exists an integer N' for which $A_{N'} \cap \mathcal{R}' = \emptyset$. Since $m < n$ implies $A_m \supseteq A_n$, we conclude that $A_N \cap \mathcal{R}' = \emptyset$ for all $N \ge N'$.

Similarly, since $\mathcal{R}''$ is a set of random elements, there exists an integer N'' for which $A_{N''} \cap \mathcal{R}'' = \emptyset$. Since $m < n$ implies $A_m \supseteq A_n$, we conclude that $A_N \cap \mathcal{R}'' = \emptyset$ for all $N \ge N''$.

For $N \stackrel{\text{def}}{=} \max(N', N'')$, we have $N \ge N'$ and $N \ge N''$ and hence, $A_N \cap \mathcal{R}' = \emptyset$ and $A_N \cap \mathcal{R}'' = \emptyset$. So, no element of A_N belongs to $\mathcal{R}'$ or to $\mathcal{R}''$. In other words, no element of A_N belongs to the union $\mathcal{R} = \mathcal{R}' \cup \mathcal{R}''$. So, $A_N \cap \mathcal{R} = \emptyset$. Lemma is proven.

Proof of Lemma 4. To prove that the union $\mathcal{T} = \mathcal{T}' \cup \mathcal{T}''$ is a set of typical elements, let us assume that A_n be a definable sequence of sets for which $A_n \supseteq A_{n+1}$ and $\cap A_n = \emptyset$. We need to prove that there exists an integer N for which $A_N \cap \mathcal{T} = \emptyset$.

Indeed, since $\mathcal{T}'$ is a set of typical elements, there exists an integer N' for which $A_{N'} \cap \mathcal{T}' = \emptyset$. Since $m < n$ implies $A_m \supseteq A_n$, we conclude that $A_N \cap \mathcal{T}' = \emptyset$ for all $N \ge N'$.

Similarly, since $\mathcal{T}''$ is a set of typical elements, there exists an integer N'' for which $A_{N''} \cap \mathcal{T}'' = \emptyset$. Since $m < n$ implies $A_m \supseteq A_n$, we conclude that $A_N \cap \mathcal{T}'' = \emptyset$ for all $N \ge N''$.

For $N \stackrel{\text{def}}{=} \max(N', N'')$, we have $N \ge N'$ and $N \ge N''$ and hence, $A_N \cap \mathcal{T}' = \emptyset$ and $A_N \cap \mathcal{T}'' = \emptyset$. So, no element of A_N belongs to $\mathcal{T}'$ or to $\mathcal{T}''$. In other words, no element of A_N belongs to the union $\mathcal{T} = \mathcal{T}' \cup \mathcal{T}''$. So, $A_N \cap \mathcal{T} = \emptyset$. Lemma is proven.

Proof of Proposition 2. Let us first prove that every two universal descriptions of randomness $\mathcal{R}_n$ and $\mathcal{R}'_n$ are equivalent to each other. Indeed, for every n, by definition of a description of randomness, the set $\mathcal{R}_n$ is a L_1-definable set of random elements. Due to the fact that the description $\mathcal{R}'_n$ is universal, there exists a natural number n' for which $\mathcal{R}_n \subseteq \mathcal{R}'_{n'}$. Similarly, we can prove that for every n', there exists a natural number n for which $\mathcal{R}_n \subseteq \mathcal{R}'_{n'}$. Equivalence is proven.

Let us now prove existence of a universal description of randomness. Indeed, in the language L_2, we can formally describe L_1-definability, so we can have a sequence $\mathcal{R}_{(1)}$, $\mathcal{R}_{(2)}$, ..., of all L_1-definable sets of random elements. Now, we can take

$$\mathcal{R}_n \stackrel{\text{def}}{=} \mathcal{R}_{(1)} \cup \ldots \cup \mathcal{R}_{(n)}.$$

Each of these sets is also L_1-definable. Due to our construction, we have $\mathcal{R}_n \subseteq \mathcal{R}_{n+1}$, so this is indeed a description of randomness.

Let us prove that this description is universal. Indeed, each L_1-definable description of randomness $\mathcal{R}$ is in the sequence $\mathcal{R}_{(1)}$, $\mathcal{R}_{(2)}$, ..., so it has the form $\mathcal{R} = \mathcal{R}_{(n)}$ for some n. Then, by definition of $\mathcal{R}_n$, we have $\mathcal{R} = \mathcal{R}_{(n)} \subseteq \mathcal{R}_n$. Universality is proven, and so it the proposition.

Proof of Proposition 3 is similar.

References

1. Li M., Vitanyi P. An Introduction to Kolmogorov Complexity and Its Applications. Berlin, Heidelberg, New York : Springer, 2008.
2. Kreinovich V., Finkelstein A.M. Towards applying computational complexity to foundations of physics // Notes of Mathematical Seminars of St. Petersburg Department of Steklov Institute of Mathematics. 2004. V. 316. P. 63–110; reprinted in Journal of Mathematical Sciences. 2006, V. 134, N. 5, P. 2358–2382.
3. Misner C.W., Thorne K.S., Wheeler J.A. Gravitation. New York : W. H. Freeman, 1973.

Mathematical Structures and Modeling
2012, N. 26, pp. 57–63

UDC 530.145:51-73

IF ENERGY IS NOT PRESERVED, THEN PLANCK'S CONSTANT IS NO LONGER A CONSTANT: A THEOREM

V. Kreinovich, A. Ortiz

For any physical theory, to experimentally check its validity, we need to formulate an alternative theory and check whether the experimental results are consistent with the original theory or with an alternative theory. In particular, to check whether energy is preserved, it is necessary to formulate an alternative theory in which energy is not preserved. Formulating such a theory is not an easy task in quantum physics, where the usual Schroedinger equation implicitly assumes the existence of an energy (Hamiltonian) operator whose value is preserved. In this paper, we show that the only way to get a consistent quantum theory with energy non-conservation is to use Heisenberg representation in which operators representing physical quantities change in time. We prove that in this representation, energy is preserved if and only if Planck's constant remains a constant. Thus, an appropriate quantum analogue of a theory with non-preserved energy is a theory in which Planck's constant can change – i.e., is no longer a constant, but a new field.

1. Formulation of the Problem

Every physical law needs to be experimentally tested. Physics is a rapidly changing science, new discoveries are being made all the time, experimental discoveries that are often inconsistent with the existing physics and which lead to a development of new physical theories. Testing the existing physical theories is one of the main ways how physics evolves.

How physical laws can be experimentally tested. To test a physical law, we must:

- formulate an alternative theory in which this law is not valid (while others are valid),
- find a testable experimental situation in which the predictions of this alternative theory differ from the predictions of the original theory, and then
- experimentally check which of the two theories is correct.

Copyright © 2012 **V. Kreinovich, A. Ortiz**
University of Texas at El Paso (USA)
E-mail: vladik@utep.edu, aortiz19@miners.utep.edu

Example. This is how the General Relativity theory (alternative at that time) was experimentally tested: by experimentally comparing the predictions of Newton's gravitation theory – the prevalent theory of that time – with the predictions of the alternative theory; see, e.g., [3].

How can we test energy conservation law? A problem. One of the fundamental physical laws is the energy conservation law. At first glance, checking this law is easy: even on the level of Newton's physics, with the usual equations of motion

$$\frac{d^2x_i}{dt^2} = \frac{1}{m} \cdot f_i, \tag{1}$$

relating acceleration $\frac{d^2x_i}{dt^2}$ with the force f_i, there are many non-potential force fields $f_i(x)$ in which energy is not preserved.

The problem appears when we take quantum effects into account, i.e., when we consider the quantum equations. In quantum physics, the main equation – originally formulated by Schroedinger – has the form (see, e.g., [1])

$$\mathrm{i} \cdot \hbar \cdot \frac{\partial \psi}{\partial t} = H\psi, \tag{2}$$

where $\mathrm{i} \stackrel{\mathrm{def}}{=} \sqrt{-1}$, $\psi(x)$ is the wave function describing the quantum state, and H is a so-called *Hamiltonian*, an operator describing the energy of a state. In a non-potential force field, there is no well-defined notion of a total energy and thus, it is not possible to write down the corresponding quantum equation.

Discussion. The need to test the energy conservation law on quantum level is not purely theoretical:

- on a pragmatic level, serious physicists considered the possibility of micro-violations of energy conservation starting from the 1920s [1];
- on a more foundational level, the intuitive ideas of free will seem to lead to possible energy non-conservation [2].

What we do in this paper. In this paper, we show how to form a quantum theory in which energy is not conserved. Specifically, we show that for quantum theories, energy non-conservation is equivalent to changing Planck's constant. Thus, in quantum physics, checking whether energy is conserved is equivalent to checking whether Planck's constant changes.

2. Analysis of the Problem

Schroedinger and Heisenberg representations of quantum physics: reminder. In quantum physics (see, e.g., [1]), states are described by elements of

a Hilbert space – e.g., of the space of all square-integrable functions $\psi(x)$ – and physical quantities are described by linear operators in this space.

Historically, quantum physics started with a description by Heisenberg, in which states are fixed but operators change. Very soon, it turned out that in most cases, an alternative representation is more computationally advantageous – a representation in which operators are fixed but states change. This representation was originally proposed by E. Schroedinger and is therefore known as the Schroedinger representation.

Since we cannot use Schroedinger's representation, we will use the Heisenberg one. As we have mentioned, the Schroedinger's equation implicitly assumes the existence of (preserved) energy. Thus, to describe situations in which energy is not preserved, it is reasonable to use the Heisenberg representation.

Heisenberg representation: first approximation. In the Heisenberg representation, physical quantities like coordinates x_i and components $p_i \stackrel{\text{def}}{=} m \cdot \dfrac{dx_i}{dt}$ of the momentum vector are represented by operators. In the first approximation, the usual quantum mechanics is described by the usual Newton's equations

$$\frac{dx_i}{dt} = \frac{1}{m} \cdot p_i, \quad \frac{dp_i}{dt} = f_i, \tag{3}$$

with the only difference that instead of scalars x_i and p_i, we now consider operators. This description was first found by P. Ehrenfest (see, e.g., [1]).

The difference between the scalars and operators is that operators, in general, do not commute, i.e., in general, for two operators a and b, we have $[a,b] \stackrel{\text{def}}{=} ab - ba \neq 0$. Specifically, in the usual quantum physics, operators x_i and x_j corresponding to different coordinates commute with each other, operators p_i and p_j commute with each other, but operators x_i and p_i do not commute:

$$[x_i, x_j] = 0, \quad [p_i, p_j] = 0, \quad [p_i, x_j] = \mathrm{i} \cdot \hbar \cdot \delta_{ij}, \tag{4}$$

where the Kronecker's delta δ_{ij} is equal to 1 when $i = j$ and to 0 otherwise. For the usual energy-preserving quantum mechanics, these commuting relations get preserved as the operators x_i and p_i change in time – in accordance with Ehrenfest equations (3).

In the first approximation, the commutator $[a,b]$ can be described in terms of the Poisson brackets (see, e.g., [1]). Namely, for arbitrary functions $a(x,p)$ and $b(x,p)$ of coordinates $x = (x_1, x_2, x_2)$ and momentum $p = (p_1, p_2, p_3)$, we have

$$[a,b] = \mathrm{i} \cdot \hbar \cdot \{a,b\} + o(\hbar), \tag{5}$$

where

$$\{a,b\} \stackrel{\text{def}}{=} \sum_k \left(\frac{\partial a}{\partial p_k} \cdot \frac{\partial b}{\partial x_k} - \frac{\partial a}{\partial x_k} \cdot \frac{\partial b}{\partial p_k} \right). \tag{6}$$

As an example, let us show what happens for the Heisenberg commutator $[a, b]$ for which $a = p_i$ and $b = x_j$. Since $a = p_i$ depends only on p_i, we have $\frac{\partial p_i}{\partial p_k} = \delta_{ik}$ and $\frac{\partial p_i}{\partial x_k} = 0$. Similarly, since $b = x_j$ depends only on x_j, we have $\frac{\partial x_j}{\partial p_k} = 0$ and $\frac{\partial x_j}{\partial x_k} = \delta_{jk}$. Thus,

$$\{p_i, x_j\} = \sum_k \delta_{ik} \cdot \delta_{jk} = \delta_{ij}.$$

When the force comes from a potential field, Planck's constant is preserved. Let us show that in the potential field with potential energy $V(x)$, when $f_i = -\frac{\partial V}{\partial x_i}$, Planck's constant is preserved. Indeed, let us assume that the commuting relations (4) hold at a certain moment of time t_0. In particular, this means that $[p_i, x_j] = \mathrm{i} \cdot \hbar \cdot \delta_{ij}$. Let us show that – at least in the first approximation – this relation is preserved, in the sense that $\frac{d}{dt}[p_i, x_j] = 0$.

First, we should note that since $[a, b] = ab - ba$, we have

$$\frac{d}{dt}([a, b]) = \frac{d}{dt}(ab - ba) = \frac{da}{dt}b + a\frac{db}{dt} - \frac{db}{dt}a - b\frac{da}{dt} = \left[\frac{da}{dt}, b\right] + \left[a, \frac{db}{dt}\right].$$

Thus, we have

$$\frac{d}{dt}([p_i, x_j]) = \left[\frac{dp_i}{dt}, x_j\right] + \left[p_i, \frac{dx_j}{dt}\right]$$

Due to Ehrenfest equations, we have $\frac{dp_i}{dt} = f_i$ and $\frac{dx_i}{dt} = \frac{1}{m} \cdot p_i$, so we have

$$\frac{d}{dt}([p_i, x_j]) = [f_i, x_j] + \frac{1}{m} \cdot [p_i, p_j]. \tag{7}$$

Since f_i depend only on the coordinates, and all coordinate operators commute, we have $[f_i, x_j] = 0$. Since all the components of the momentum commute, we have $[p_i, p_j] = 0$. Thus, we conclude that $\frac{d}{dt}([p_i, x_j]) = 0$.

Similarly, we can conclude that the second derivative of the Heisenberg commutator is also equal to 0. Indeed, by differentiating both sides of the equation (7), we conclude that

$$\frac{d^2}{dt^2}([p_i, x_j]) = \left[\frac{df_i}{dt}, x_j\right] + \frac{1}{m} \cdot [f_i, p_j] + \frac{1}{m} \cdot [f_i, p_j] + \frac{1}{m} \cdot [p_i, f_j]. \tag{8}$$

Here, since f_i depends only on coordinates, we have

$$\frac{df_i}{dt} = \sum_\ell \frac{\partial f_i}{\partial x_\ell} \cdot \frac{dx_\ell}{dt} = \frac{1}{m} \cdot \sum_\ell \frac{\partial f_i}{\partial x_\ell} \cdot p_\ell,$$

so

$$\frac{d^2}{dt^2}([p_i, x_j]) = \frac{1}{m} \cdot \left(\left[\sum_\ell \frac{\partial f_i}{\partial x_\ell} \cdot p_\ell, x_j \right] + 2[f_i, p_j] + [p_i, f_j] \right).$$

Thus, to prove that this second derivative is equal to 0, it is sufficient to prove that the expression in parentheses is equal to 0. In the first approximation, this expression is proportional to the sum S of the corresponding Poisson brackets

$$S = \left\{ \sum_\ell \frac{\partial f_i}{\partial x_\ell} \cdot p_\ell, x_j \right\} + 2\{f_i, p_j\} + \{p_i, f_j\};$$

so, in the first approximation, it is sufficient to prove that the sum S is equal to 0. In the first bracket, x_j depends only on x_j, so

$$\left\{ \sum_\ell \frac{\partial f_i}{\partial x_\ell} \cdot p_\ell, x_j \right\} = \sum_k \sum_\ell \frac{\partial f_i}{\partial x_\ell} \cdot \delta_{k\ell} \cdot \delta_{jk} = \frac{\partial f_i}{\partial x_j}.$$

For the second term of the sum S, since p_j only depends on the momentum, we get

$$\{f_i, p_j\} = -\sum_k \frac{\partial f_i}{\partial x_k} \cdot \delta_{jk} = -\frac{\partial f_i}{\partial x_j}.$$

Similarly,

$$\{p_i, f_j\} = \frac{\partial f_j}{\partial x_i}.$$

Thus, we have

$$S = \frac{\partial f_j}{\partial x_i} - \frac{\partial f_i}{\partial x_j}.$$

For the potential field, we have $f_i = -\dfrac{\partial V}{\partial x_i}$ and therefore,

$$\frac{\partial f_i}{\partial x_j} = -\frac{\partial^2 V}{\partial x_i \partial x_j}.$$

Hence, we have

$$S = -\frac{\partial^2 V}{\partial x_i \partial x_j} + \frac{\partial^2 V}{\partial x_i \partial x_j} = 0.$$

What happens when energy is not preserved: an example. We are interested in situations where energy is not preserved. Let us start our analysis with the simplest such situation of the friction force $f_i = -k \cdot v_i$, i.e., force of the type $f_i = -k_0 \cdot p_i$, where $k_0 \stackrel{\text{def}}{=} \dfrac{k}{m}$. In this case, from the formula

$$\frac{d}{dt}([p_i, x_j]) = [f_i, x_j] + \frac{1}{m} \cdot [p_i, p_j],$$

by using $[p_i, p_j] = 0$, we get

$$\frac{d}{dt}([p_i, x_j]) = -k_0 \cdot [p_i, x_j].$$

In other words, for $h \stackrel{\text{def}}{=} [p_i, x_i]$, we have a differential equation

$$\frac{dh}{dt} = -k_0 \cdot h.$$

From this equation, we conclude that $\frac{dh}{h} = -k_0 \cdot dt$ hence $\ln(h) = \text{const} - k_0 \cdot t$, and $h(t) = \text{const} \cdot \exp(-k_0 \cdot t)$. We know that $h(t_0) = \mathrm{i} \cdot \hbar$, hence

$$h(t) = h(t_0) \cdot \exp(-k_0 \cdot (t - t_0)).$$

At the initial moment t_0, we have $h(t_0) = \mathrm{i} \cdot \hbar$. So, the above equation means, in effect, that Planck's constant $\hbar \stackrel{\text{def}}{=} \frac{[p_i, x_i]}{\mathrm{i}}$ is no longer a constant – it exponentially decreases with time.

Discussion. Let us show that the same phenomenon – of Planck's constant no longer being a constant – occurs for every theory in which energy is not preserved.

3. Main Result

Formulation of the main result. Let us consider the general case, when each component f_i of a force is a function of coordinates x and momentum p. We will show that if in the quantum version of this theory, Planck's constant remains a constant, i.e., we have $[p_i, x_j] = \mathrm{i} \cdot \hbar \cdot \delta_{ij}$ for all moments of time, then the field f_i is a potential field, i.e., has the form $f_i = -\frac{\partial V}{\partial x_i}$ for some function $V(x)$.

This means that if f_i is *not* a potential field, then Planck's constant is no longer a constant.

Proof. If Planck's constant is a constant, this means, in particular, that we have $\frac{d}{dt}([p_i, x_j]) = 0$. Explicitly differentiating the left-hand side, we conclude that $[f_i, x_j] + \frac{1}{m} \cdot [p_i, p_j] = 0$. Since $[p_i, p_j] = 0$, we get $[f_i, x_j] = 0$. In the first approximation, this means that the corresponding Poisson bracket is equal to 0: $\{f_i, x_j\} = 0$. Since x_j depends only on the coordinate, we get

$$\{f_i, x_j\} = \sum_k \frac{\partial f_i}{\partial p_k} \cdot \delta_{kj} = \frac{\partial f_i}{\partial p_j} = 0.$$

The fact that all partial derivatives of f_i relative to p_j are equal to 0 means that f_i does not depend on the momentum. In other words, the force f_i depends only on the coordinates x.

Now, since we know that f_i depend only on the coordinates, for the second time derivative $\frac{d^2}{dt^2}([p_i, x_j])$, we can repeat arguments from the previous section and conclude that in the first approximation, this second derivative is proportional to

$$S = 2 \cdot \frac{\partial f_i}{\partial x_j} - 2 \cdot \frac{\partial f_i}{\partial x_j}.$$

So, from the fact that the second derivative is equal to 0, we conclude that $S = 0$, i.e., that

$$\frac{\partial f_i}{\partial x_j} = \frac{\partial f_i}{\partial x_j}$$

for all i and j. It is known that these equalities are necessary and sufficient conditions for the existence of a field V for which $f_i = -\frac{\partial V}{\partial x_i}$. Thus, we have proved that f_i is indeed a potential field. ■

Discussion. Theories in which Planck's constant is no longer a constant but a new physical field $s(x)$ have been proposed; see, e.g., [4].

It should be mentioned that we may need to go beyond proposed theory: indeed, these theories only consider a *scalar* field $s(x)$ corresponding to

$$[p_i, x_j] = \mathrm{i} \cdot \hbar \cdot s(x) \cdot \delta_{ij},$$

while, in general, the commutator $[p_i, x_j]$ can be an arbitrary *tensor*.

Acknowledgments

This research was partly supported by the National Science Foundation grants HRD-0734825 and HRD-1242122 (Cyber-ShARE Center of Excellence) and DUE-0926721, by Grant 1 T36 GM078000-01 from the National Institutes of Health, and by a grant on F-transforms from the Office of Naval Research.

One of the authors (VK) is greatly thankful to his late father Yakov R. Kreinovich for inspiring ideas and discussions about energy conservations.

References

1. Feynman R., Leighton R., Sands M. The Feynman Lectures on Physics. Boston, Massachusetts : Addison Wesley, 2005.
2. Kreinovich V. In quantum physics, free will leads to nonconservation of energy // Journal of Uncertain Systems. 2013. V. 7, to appear.
3. Misner C.W., Thorne K.S., Wheeler J.A. Gravitation. New York : W. H. Freeman, 1973.
4. Phipps T.E. Jr. // Found. Phys. 1973. V. 3. P. 435.

Математические структуры и моделирование
2012, вып. 26, с. 64–72

УДК 530.1:159.963:51-7

МОДЕЛЬ СМЕНЫ СОЗНАНИЯ СНА И СОЗНАНИЯ РЕАЛЬНОСТИ

А.К. Гуц

Даётся математическое описание сна, в котором, по мнению Флоренского, наблюдается течение времени в обратном направлении.

Под обращением времени, как правило, понимают его течение вспять, т.е. от будущего к прошлому. Считается, что это невозможно. Во всяком случае CPT-теорема говорит, обращение времени должно сопровождаться зеркальным отражением и заменой частиц на античастицы. Вряд ли это то, чего хотели бы те, кто пишет об обращении времени.

Но Флоренский нашёл ситуацию, связанную со сном человека, которая явно нам указывает на обратное течение времени во сне. Рассмотрим подробнее пример, данный Флоренским, и покажем, что описанная в нём ситуация вполне может быть адекватно и непротиворечиво описана математически.

1. Два потока времени, обнаруженные Павлом Флоренским

Флоренский обратил внимание на явную корреляцию событий реальности и сна, не допускающую причинно-следственного объяснения [1, с. 7–17]:

> «Сонная фантазия представляет нам ряд лиц, местностей и событий, целесообразно сцепляющихся между собою, т.е., конечно, не глубокой осмысленностью событий, которыми направляется действие сонной драмы, а — в смысле прагматизма: мы ясно сознаем связь, приводящую от некоторых причин, событий-причин, видимых во сне, к некоторым следствиям, событиям-следствиям сновидения; отдельные события, как бы ни казались они нелепыми, однако связаны в сновидении причинными связями, и сновидение развивается, стремясь в определённую сторону, и роковым, — с точки зрения сновидца, — роковым образом приводит к некоторому заключительному событию, являющемуся развязкою и завершением всей системы последовательных причин и следствий. Сновидение завершается событием x, которое произошло потому, что раньше его произошло событие t, а t произошло потому, что раньше его было событие s, а s имело

Copyright © 2012 **А.К. Гуц**
Омский государственный университет им. Ф.М. Достоевского
E-mail: guts@omsu.ru

прежде себя свою причину r и т.д. и т.д., восходя от следствий к причинам, от последующего к предыдущему, от настоящего к прошедшему до некоторого начального и обыкновенно совсем незначительного, ничем не знаменательного события α — причины всего последующего за ним, как это сознается в сновидении. Но мы помним ведь, что причиною извне, дневным сознанием наблюдаемою, всего сновидения, как целого, как целой композиции, было некоторое внешнее, для замкнутой системы спящего, событие или обстоятельство. Назовём его Ω. Теперь, спящий просыпается, не только побуждённый этою причиною Ω к бывшему у него сновидению, но и пробуждённый им, причём, однако, развязка сновидения, x, совпадает, или почти совпадает, по своему содержанию с переживаемою наяву причиною сновидения Ω. Это совпадение бывает обычно настолько точно, что и в голову не придёт усомниться в непосредственности связи события x и причины Ω: развязка сновидения, несомненно, есть сонная перефразировка некоторого события внешнего мира Ω, вторгнувшегося в уединённый от всего внешнего мир спящего. Если я вижу сон, в котором происходит выстрел, а в комнате возле меня на самом деле был выстрел или хлопнули дверью, то может ли быть сомнение в *неслучайности* такого сновидения: ну, конечно, выстрел в сновидении есть духовный отголосок на выстрел во внешнем мире. Если угодно, тот и другой выстрел есть двоякое восприятие — ухом сонным и ухом бодрствующим — одного и того же физического процесса. Или во сне я увижу множество душистых цветов, тогда как мне поднесли к носу флакон с духами, то опять было бы неестественно подумать на случайность совпадения двух запахов: запаха во сне — цветочного — и запаха внешне обоняемого — духов. Если во сне мне навалился кто-то на грудь и стал душить меня, а когда от страха я проснулся, то этот навалившийся оказался, положим, подушкою, попавшею мне на грудь; или если меня укусила собака в сновидении, а, проснувшись от ощущения этого укуса, я обнаружил, что меня в самом деле ужалило влетевшее в открытое окно насекомое, то и тут и в бесчисленном множестве других подобных же случаев совпадение развязки x с причиной сновидения Ω никак не случайно.

Мы можем только согласиться о наличии корреляции между x и Ω, но не с содержанием события x. Ведь x в случае, если Ω — хлопок двери, — это и выстрел x_1, и звук удара доски о пол x_2, и звук сломавшейся ветки x_3, и многое многое другое. Имеет смысл принять, что под x следует понимать семейство событий $\{x(b)\}_{b\in\mathbb{R}}$.

Повторяем, одно и то же действительное событие воспринимается по *двум* сознаниям: в дневном сознании — как Ω, а в ночном — как x.

Важный момент: Флоренский вводит в рассмотрение два сознания — дневное и ночное.

По-видимому, во всем сказанном нет ничего особенного; да, не было *бы*, если *бы* событие x, будучи следствием Ω, т.е., входя в ряд дневной, внешней причинности, не участвовало вместе с тем в *другом* причинном ряде

— причинности *ночного* сознания и не было тоже следствием, но совсем не той причины, мало того, целого ряда причин и следствий, нисходящих крепко спаянною цепью к некоторой начальной причине α. Между тем, α заведомо не имеет по содержанию ничего общего с причиной Ω и, следовательно, не могло быть ею вызвано. А если бы не было α со всеми происходящими из него следствиями, то не было бы и всего сновидения, т.е. не могло бы быть развязки x, т.е. мы не проснулись бы и, следовательно, внешняя причина Ω не дошла бы до нашего сознания. Итак, несомненно: x есть отражение сонною фантазиею явления Ω, но x не есть deus ex machina[1] без всякого смысла, вопреки логике и ходу событий в сновидении вторгающееся во внутренние образы и бессмысленно их обрывающее, а действительно составляет развязку некоторого драматического действия.

Иначе говоря, любое яйцо x имеет курицу α, которая его снесла, и внешний толчок Ω, принявший во сне, в ночном сознании форму события x, запускает в ночном сознании цепочку-действие, начинающегося с «курицы» α, которая живёт и в какой-то последующий конечный миг, совпадающий с пробуждением человека, т.е. со сменой ночного сознания на дневное, производящей на свет «яйцо» x.

Дело со сновидением происходит совсем не так, как мыслят о жизни не чувствующие Провидения, когда крушение поезда или выстрел из-за угла прекращает развёртывающуюся и много обещающую деятельность, а — так именно, как в превосходной драме, в которой конец приходит потому, что вызрели все подготовлявшие его события, и было бы нарушением смысла и цельности всей драмы, если бы развязки не произошло. Никоим образом, учитывая крепчайшую прагматическую связность между собою всех событий сновидения, мы не можем усматривать в развязке x события самостоятельного, извне подклеенного к ряду прочих событий и по какой-то непостижимой случайности не нарушающего внутренней логики и художественной правды сновидения во всех его деталях. Нет сомнения, сновидения разбираемого типа суть целостные, замкнутые в себе единства, в которых конец, развязка, предусматривается с самого начала и, более того, собою определяет и начало, как завязку, и все целое. Принимая же во внимание малозначительность завязки $[^{-}x^{-}]$ самой по себе, без завершающих ее последствий, как это вообще бывает в крепко сделанной драме, мы имеем полное право утверждать телеологичность *всей* композиции сновидения: все его события развиваются в виду развязки, для того, чтобы развязка не висела в воздухе, не была несчастной случайностью, но имела глубокую прагматическую мотивировку.

<..>

Если, например, в сновидении, облетевшем все учебники психологии, спящий пережил чуть ли не год или более французской революции, присутствовал при самом её зарождении и, кажется, участвовал в ней, а затем, после долгих и сложных приключений, с преследованиями и погонями,

[1] Бог из машины (лат.).

террора, казни Короля и т.д. был наконец, вместе с жирондистами, схвачен, брошен в тюрьму, допрашиваем, предстоял революционному трибуналу, был им осуждён и приговорён к смертной казни, затем привезён на телеге к месту казни, возведён на эшафот, голова его была уложена на плаху и холодное острие гильотины уже ударило его по шее, причём он в ужасе проснулся, — то неужели придёт на мысль усмотреть в последнем событии — прикосновении ножа гильотины к шее — нечто *отдельное* от всех прочих событий? и неужели все развитие действия — от самой весны революции и включительно до возведения видевшего этот сон на эшафот — не устремляется сплошным потоком событий именно к этому завершительному холодному прикосновению к шее, — к тому, что мы назвали событием x? — Конечно, такое предположение совершенно невероятно. А между тем видевший всё описываемое проснулся *от того*, что спинка железной кровати, откинувшись, с силой ударила его по обнажённой шее. Если у нас не возникает сомнений во *внутренней* связности и цельности сновидения от начала революции (α) до прикосновения ножа (x), то тем менее может быть сомнений, что ощущение во сне холодного ножа (x) и удар холодным железом кровати по шее, когда голова лежала на подушке (Ω), есть *одно и то же явление*, но воспринятое двумя различными сознаниями. И, повторяю, тут не было бы ничего особенного, если *бы* удар железом (Ω) разбудил спящего и вместе с тем во время, вообще недолгого, просыпания облёкся в символический образ хотя бы того же самого удара гильотинным ножом, а этот образ, амплифицируясь ассоциациями, хотя бы на ту же тему французской революции, развернулся в более или менее длинное сновидение. Но все дело в том, что сновидение это, как и бесчисленные прочие того же рода, протекает *как раз наоборот против того*, как мы могли бы ждать, помышляя о кантовском времени. Мы говорим: внешняя причина (Ω) сновидения, которое составляет одно целое, есть удар железом по шее, и этот удар символизируется непосредственно в образе прикоснувшегося гильотинного ножа (x). Следовательно, духовная причина всего сновидения есть это событие x. Следовательно, в дневном сознании, по схеме дневной причинности, оно и по времени должно предшествовать событию α, духовно происходящему из события x. Иначе говоря, событие x во времени видимого мира должно быть завязкою сновидческой драмы, а событие a — её развязкою. Тут же, во времени мира невидимого, происходит навыворот, и причина x появляется не прежде своего следствия a, и вообще не прежде всего ряда следствий своих $b, c, d, ..., r, s, t$, а *после* всех них, завершая весь ряд и определяя его не как причина действующая, а как *причина конечная* — $\tau\acute{\varepsilon}\lambda o\varsigma$.

2. Математическая модель дневного и ночного сознания-времени

В книге [2, Часть III] предложена модель *оживления* вневременного формального пространства-времени Минковского-Витгенштейна $\langle R^4, g_{ik}^{(4)} \rangle$, где R^4 декартово произведение коммутативного кольца R, удовлетворяющего набору аксиом, главной из которых является аксиома Кока-Ловера, означающая, что

теория с необходимостью должна описываться в рамках интуиционистской логики (см. [2]).

Формальное пространство-время R^4, как и его классический аналог, статично, т.е. вневременно, не содержит времени.

Событие x в таком пространстве-времени есть «мировая точка» $x = (x^0, x^1, x^2, x^3) \in R^4$, задаваемая в координатах соотношениями:

$$\begin{cases} x^0 = ct, \\ x^1 = lx, \\ x^2 = ly, \\ x^3 = lz, \end{cases} \tag{1}$$

где константа l введена нами на основе простой (но отнюдь не наивной[2]) мысли о необходимости симметричной записи события x временной координаты x^0 и пространственных координат x^α $(\alpha = 1, 2, 3)$.

Формальное пространство-время R^4 интерпретируется как объект топоса:

$$R^4 = \ell C^\infty(\mathbb{R}^4) \in \mathbf{Sets}^{\mathbf{L^{op}}},$$

где $\mathbf{L}$ — это дуальная категория для категории конечно порождённых C^∞-колец, имеющих вид $A = C^\infty(\mathbb{R}^m)/I$, где I — конечно порождённый идеал. Она называется *категорией локусов*. Объектами категории $\mathbf{L}$ являются всё те же конечно порождённые C^∞-кольца, а морфизмами — обращённые морфизмы категории конечно порождённых C^∞-колец. Во избежание путаницы принято объекты (локусы) категории $\mathbf{L}$ обозначать как ℓA, где A — C^∞-кольцо.

Таким образом, R^4 является уже не простым набором точек, но набором гладких функций.

Предположим, что константы c, l складываются из «классического значения» c_0 и l_0 соответственно и бесконечно малых слагаемых, т.е.

$$c = c_0 + d, \quad l = l_0 + \delta,$$

где $c_0 = 3 \cdot 10^{10}$ *см/сек* и $l_0 = 10^{-33}$ *см*. Тогда при интерпретации в гладком топосе $\mathbf{Sets}^{\mathbf{L}^{op}}$ бесконечно малые слагаемые $d, \delta \in D$ в стадии $\ell A = \ell C^\infty(\mathbb{R}^m)/I$ представляются гладкими функциями $d(a), \delta(a)$, где $a \in \mathbb{R}^m$, такими, что $d^2, \delta^2 \in I$.

Следовательно, событие x в стадии ℓA или, в иных терминах, обобщённый элемент $x \in_{\ell A} R^4$ задаётся соотношениями вида:

$$\begin{cases} x^0 = [c_0 + d(a)]t, \\ x^1 = [l_0 + \delta(a)]x, \\ x^2 = [l_0 + \delta(a)]y, \\ x^3 = [l_0 + \delta(a)]z. \end{cases} \tag{2}$$

[2]Константу l в физике называют фундаментальной константой длины или константой Планка.

Событие x — не пустое место, оно наполнено, как писал Минковский, *субстанцией*. Следовательно, x — это субстанция-вещь, субстанция-объект, субстанция-явление.

При изменении параметров «наблюдения» $a \in \mathbb{R}^m$ субстанции-объекта x, описываемого как (вне(шне))физическое *поле* с компонентами $d(a), \delta(a)$, событие x размазывается по пространству-времени, теряет свой точечный характер. Это означает *начало движения объекта x, начало течения времени*.

Научный подход к описанию субстанции **требует предъявления уравнений**, которым должны удовлетворять поля $d(a), \delta(a)$. По своему смыслу это уравнения как для физических констант c и l, так и способа наблюдения объектов, помещаемых в Мир событий, лишённый времени. Следовательно, в равной мере это *уравнения для времени*. Такие уравнения действительно могут быть предъявлены. Как это делается, показано в [2, 3].

2.1. Дневное и ночное сознание-время

Мы считаем, что сознание, а значит и время, — это выбор стадии и соответствующее представление явления-события x во времени, связанном с рассматриваемой стадией.

Таким образом, если дневное сознание (всех людей) — это, например, просмотр события x в стадии $\ell A = \ell C^\infty(\mathbb{R})/I$, т.е. $d = d_1(a)$, а ночное (для всех людей) — стадия $\ell B = \ell C^\infty(\mathbb{R})/J$, т.е. $d = d_2(b)$, то, поскольку спящий человек стоит на месте $(x^1, x^2, x^3 = const)$, течение дневного времени a или течение ночного времени (во сне) b дают одну и ту же (как множество) мировую линию $x^0 = x^0(a)$ или $x^0 = x^0(b)$:

$$\begin{cases} x^0 = [c_0 + d_1(a)]t, \\ x^1 = l_0 x \\ x^2 = l_0 y \\ x^3 = l_0 z. \end{cases} \quad \text{или} \quad \begin{cases} x^0 = [c_0 + d_2(b)]t, \\ x^1 = l_0 x \\ x^2 = l_0 y \\ x^3 = l_0 z. \end{cases}$$

Эти мировые линии всего лишь проекции кривых $x^0 = x^0(a)$ или $x^0 = x^0(b)$ в конфигурационных гиперпространствах

$$\langle R^4_{\ell A}, g^{(4)}(\ell A)\rangle \equiv \langle \mathbb{R}^5, g^{(4)}(\ell A)\rangle \quad \text{или} \quad \langle R^4_{\ell B}, g^{(4)}(\ell B)\rangle \equiv \langle \mathbb{R}^5, g^{(4)}(\ell B)\rangle,$$

$$g^{(4)}(\ell A) = g^{(4)}_{ik}(x, a)dx^i dx^k - da^2, \quad g^{(4)}(\ell B) = g^{(4)}_{ik}(x, b)dx^i dx^k - db^2,$$

для которых при выявлении зависимости метрики $g^{(4)}$ от «скрытых» параметров a или b, видимо, необходимо либо применять многомерные уравнения Эйнштейна, либо проводить варьирование по физическим константам (см. [2, § 9.13]).

Гиперпространства $R^4_{\ell A}$ — это виртуальные среды, т.е. способы существования, способы жизни вещей во временах-сознаниях, определяемых всевозможными стадиями ℓA:

$$R^4 = \sum_{\ell A \in \mathbf{L}} R^4_{\ell A} = \mathbb{R}^4 + \sum_{\ell A \in \mathbf{L},\ \ell A \neq \mathbf{1}} R^4_{\ell A},$$

где $R^4_{\mathbf{1}}, \mathbf{1} = \ell C^\infty(\mathbb{R})/(a)$ — среда, отождествляемая с классическим абсолютным Миром Минковского $\mathbb{R}^4$, который является вневременностью.

В предложенной модели явление сна с точки зрения дневного (стадия ℓA) и ночного сознания (стадия ℓB) изображено на рис. 1.

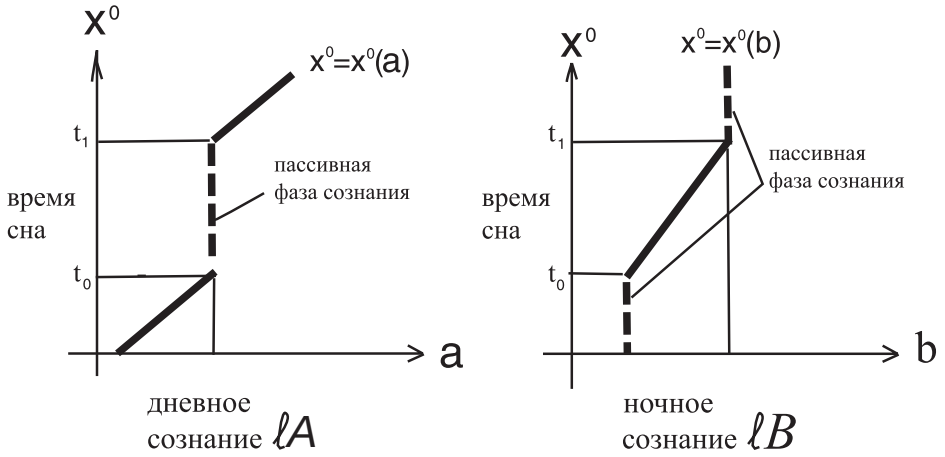

Рис. 1. Смена сознания. В пассивной фазе сознания функции $x^0 = x^0(a)$ или $x^0 = x^0(b)$ имеют конечный скачок — одно сознание «отключается», уступая место другому

Вернёмся к цитируемому тексту Флоренского с описанием сна, вызванного причиной Ω.

> Таким образом, в сновидении время бежит, и ускоренно бежит, *навстречу* настоящему, *против* движения времени бодрственного сознания. Оно *вывернуто через себя*, и, значит, вместе с ним вывернуты и все его конкретные образы. А это значит, что мы перешли в область *мнимого пространства*.

Внешнее событие Ω приводит к тому, что возникает в ночном сознании определённая ассоциация, приводящая к просмотру сна $x^0 = x^0(b)$ (см. рис. 2). На рисунке дан 5-мерный световой конус в гиперпространстве сна $R^4_{\ell B}$; его положение в осях показывает, что сон $x^0 = x^0(b)$ представляется времениподобной линией, и таковой является также кривая ассоциации в полосе $[b_0, b]$. Хотя при этом в полосе $[b_0, b]$ движение от Ω к α в проекции на временную ось x^0 формального пространства-времени идёт в направлении обратного течения времени x^0. Другими словами, это как раз то обратное течение времени во сне, о котором говорил Флоренский. Но в нашей модели время во сне не обращается, течёт оно правильно, оставаясь в 5-мерном световом конусе. Происходят всего лишь проходы туда-сюда в формальном пространстве-времени, которое является Миром событий Минковсого, существующих вечно и неизменно, но сознание может просматривать их, скользить по ним в любом направлении.

Поскольку, как мы отмечали, событие Ω может быть связано не только с одним конкретным событием во сне x, а с целым рядом событий $x_1, x_2, ..., x_n, ...$, то вместо описания сна, отражённого на рис. 2, следует рассматривать более сложную его модель, показанную на рис. 3. Эта модель говорит о том, что, видимо, Ω, вызывает не один сон, а серию параллельных снов.

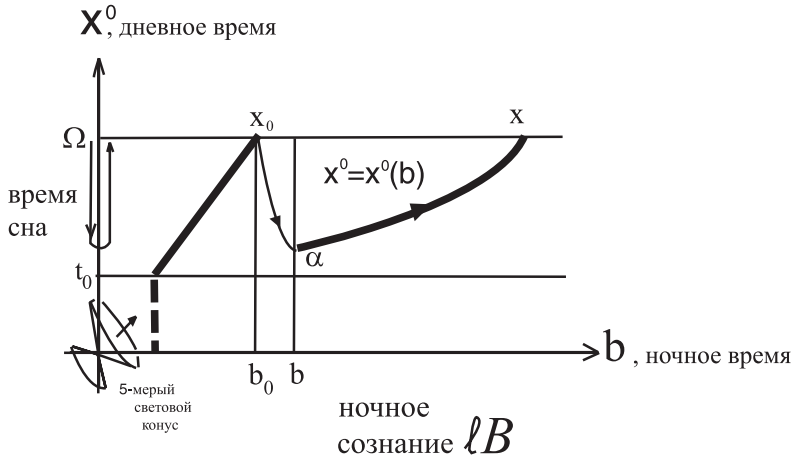

Рис. 2. Событие Ω в ночном сознании — это событие x_0 в момент b_0 времени, текущем во сне в ночном сознании. Событие x_0 ассоциируется в ночном сознании с цепочкой-действием и $x^0 = x^0(b)$, имеющим началом событие α и концом событие x. Поиск ассоциации (ассоциация) — это процесс, идущий в потоке времени, времени сна ℓB, но против потока дневного времени, времени физической реальности ℓA

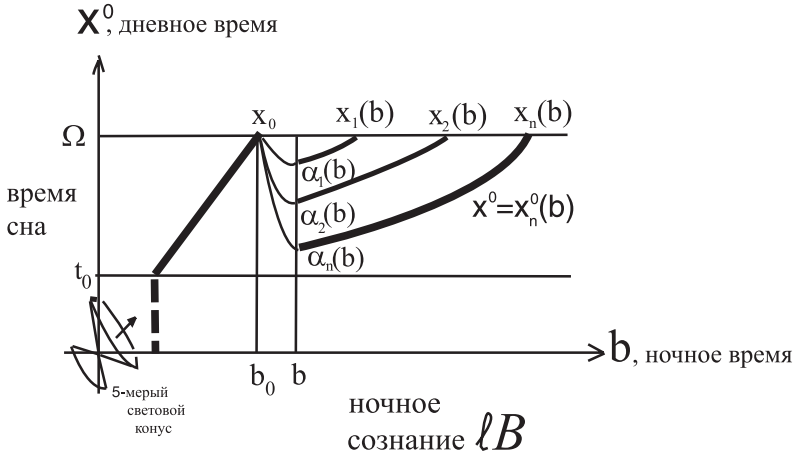

Рис. 3. Событие x_0 может вызвать множество ассоциаций. Одна их них — это сон, скажем, $x^0 = x^0_n(b)$, который вспоминается. А остальные сны? Видит ли их человек?

2.2. Переходы между явью и сном

Переход от яви к сну — засыпание — это замена среды $R^4_{\ell A}$ на среду $R^4_{\ell B}$, замена стадии ℓA на стадию ℓB, и описывается она как морфизм между стадиями

$$\ell B \xrightarrow{\Phi} \ell A.$$

Морфизм Φ осуществляет переход от гиперпространства (среды) $R^4_{\ell A}$ к гиперпространству (среде) $R^4_{\ell B}$. Убедимся в этом.

Пусть, например, $\ell A = \ell C^\infty(\mathbb{R}^n)$ и $\ell B = \ell C^\infty(\mathbb{R}^m)$. Тогда переход Φ между

стадиями даётся гладким отображением

$$\phi : \mathbb{R}^m \ni b \to a \in \mathbb{R}^n,$$

$$a = \phi(b).$$

В таком случае метрика

$$g^{(4)}_{ik}(x^0, ..., x^3, a)dx^i dx^k - da^2$$

гиперпространства $R^4_{\ell A}$ преобразуется в метрику

$$g^{(4)}_{ik}(x^0, ..., x^3, \phi(b))dx^i dx^k - [d\phi(b)]^2$$

гиперпространства $R^4_{\ell B}$.

> А это значит, что мы перешли в область *мнимого пространства*. Тогда то же самое явление, которое воспринимается отсюда — из области действительного пространства — как действительное, оттуда — из области мнимого пространства — само зрится мнимым, т.е., прежде всего, протекающим в телеологическом времени, как *цель*, как предмет стремлений. И напротив, то, что есть цель при созерцании *отсюда* и, по нашей недооценке целей, представляется нам хотя и заветным, но лишённым энергии, — *идеалом*, — оттуда же, при другом сознании, постигается как живая энергия, формующая действительность, как творческая форма жизни. Таково вообще внутреннее время органической жизни, направляемое в своём течении от следствий к причинам-целям. Но это время обычно тускло доходит до сознания.

Литература

1. Флоренский П.А. Иконостас. М. : АСТ, 2001.
2. Гуц А.К. Элементы теории времени. М. : Издательство ЛКИ, 2011.
3. Гуц А.К. Хроногеометрия. Омск : ООО «УниПак», 2008.

Математические структуры и моделирование
2012, вып. 26, с. 73–88

УДК 004.428:519.684

ОБЗОР ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ ПЛАТФОРМ ДЛЯ ГРАФИЧЕСКИХ УСКОРИТЕЛЕЙ

А.В. Багма

В статье рассматриваются основные платформы для высокопроизводительных вычислений на графических ускорителях, их основные особенности и характеристики.

Введение

Графические ускорители становятся одной из главных движущих сил в высопроизводительных компьютерных вычислениях. Они используются как в национальных, так и в коммерческих установках суперкомпьютеров. Благодаря им появляется такое понятие как персональный суперкомпьютер, что меняет смысл самого этого понятия. Появляются новые системы, языки и средства разработки, позволяющие использовать графические ускорители для построения систем различной сложности.

На текущий момент существует сравнительно большое количество библиотек, позволяющих производить вычисления на графических ускорителях. Среди наиболее известных и часто используемых можно назвать CUDA от nVidia, OpenCL, разрабатываемый Khronos Group, Stream как собственная разработка AMD, а также наборы библиотек, позволяющие программировать видеокарты с использованием языка Fortran.

CUDA — параллельная вычислительная архитектура и программная модель, разрабатываемая компанией nVidia. Архитектура CUDA включает в себя сборочный язык (assembly language) PTX и технологию сборки, на которой основывается множество параллельных языков и API интерфейсы, встроенные в графические ускорители nVidia, включая C (C++) для CUDA, OpenCL, Fortran и DirectX Compute shaders.

C для CUDA использует стандартный C с расширениями и использует возможности техники, которые недоступны в традиционном OpenCL или Direct3D (за исключением вычислительных возможностей шейдеров). Наиболее важной из этих возможностей является разделяемая память, которая позволяет значительно увеличить производительность приложений с ограниченной пропускной

Copyright © 2012 **А.В. Багма**
Омский государственный университет им. Ф.М. Достоевского
E-mail: abagma@live.com

способностью и плавающих вычислений с двойной точностью. Также важной особенностью является возможность использования произвольной модели загрузки и хранения информации, что позволяет осуществить реализацию алгоритмов, невозможную, либо весьма затруднённую ранее.

Stream — технология от ATI. Это набор аппаратных и программных средств и технологий, который позволяет графическим процессорам AMD работать совместно с центральным процессором для ускорения множества приложений, не ограничивающихся графикой. Это позволяет создавать реализации тех или иных задач, работающие со значительно большей скоростью.

OpenCL — первый открытый свободный стандарт для параллельного программирования разнородных систем. OpenCL предоставляет универсальную программную среду для разработчиков программного обеспечения для создания эффективного и переносимого кода для высокопроизводительных серверов, настольных систем и портативных устройств. Стандарт позволяет использовать разнородную смесь многоядерных центральных процессоров, графических ускорителей, Cell архитектуры и других параллельных процессоров вроде DSP.

1. CUDA

Платформа CUDA используется практически повсеместно и на данный момент фактически является стандартом. Особенностью технологии является её доступность для чрезвычайно широкого круга платформ. Использовать её возможно практически везде, начиная с персонального компьютера и заканчивая суперкомпьютерными системами. Также с использованием технологии связано возникновение нового класса гибридных CPU-GPU серверов. В качестве примера можно привести Super Micro 14 GPU Server и Ball Bullx Blade Enclosure.

Одной из причин широкого распространения данной платформы является чрезвычайно высокое отношение производительности к стоимости. Графический процессор nVidia Tesla C2050 имеет 448 вычислительных элементов, достигает пиковой производительности в 515 GFLOP/сек. для вычислений с плавающей точкой двойной точности и до 1030 GFLOP/сек. для вычислений одинарной точности [1].

Для технологии характерно разнородное программирование — использование различных процессоров для различных задач. Одной из причин подобного разделения является различие в функциональных возможностях работающих в системе процессоров. Процессоры, используемые в графических ускорителях, специализированы и слабо подходят для обеспечения внешнего взаимодействия системы. Основной отличительной особенностью технологии CUDA является её неразрывная связь с продукцией nVidia. Технология поддерживает открытый стандарт OpenCL, но использует более тесную связь с GPU от nVidia и учитывает специфические особенности аппаратного обеспечения данного производителя. Это позволяет несколько расширить и улучшить работу на соответствующих графических ускорителях.

Технология как таковая влючает в себя набор библиотек и средств разработки, адаптированных для использования с различными языками программи-

рования и платформами. В настоящий момент система содержит следующие библиотеки: CUDA C — базовая платформа для разработки приложений на C/C++, включающая драйвер с поддержкой стандарта OpenCL. На основе этой библиотеки происходит реализация вычислительных возможностей CUDA на других языках.

Технология Direct Compute предоставляет пользовательский интерфейс вычислений на графических ускорителях. Данная технология разрабатывается Microsoft и поддерживает все CUDA совместимые архитектуры графических ускорителей, начиная с G80 (DX10 и DX11).

Среди средств разработки на фортране следует отметить следующие библиотеки и системы разработки: CUDA Fortran, PCI Accelerator, NOAA Fortran buildings (ftoc), Flagon. Также существуют решения для других платформ: Python, Java, .Net — это pyCUDA, JaCUDA, CUDA.Net и BSGP. Кроме того существует огромное количество портов на сторонние платформы. Cublas — CUDA Accelerate Basic Linear Algebra Subprogramms — библиотека подпрограмм для матриц и векторов в пространстве памяти графического ускорителя, заполнения объектов данными, вызов последовательностей функций и получение данных из GPU. Среди возможностей библиотеки можно выделить вычисления как с одинарной, так и с двойной точностью, комплексные вычисления с одинарной точностью.

CUFFT (CUDA FFT) — библиотека, предназначенная для параллельных вычислений FFT (Fast Fourier Transform) на графических устройствах от nVidia. Использует «плановую» (plans like) FFTW. План содержит информацию об оптимальной конфигурации для переданной трансформации. План может быть постоянным для предотвращения повторных вычислений, что может оказаться весьма полезным, особенно учитывая, что различные типы преобразований могу потребовать различных конфигураций потоков, блоков и ядер.

Библиотекой поддерживаются 1-о, 2-х и 3-х мерные трансформации комплексных и действительных данных. Возможности пакетной обработки позволяют выполнять множество одномерных трансформаций параллельно. Допустимый размер одномерной трансформации можеть достигать 8 миллионов элементов. 2-х и 3-х мерные трансформации допускают размеры от 2-х до 16384 элементов.

MAGMA (Matrix Algebra on GPU and Multicore Architectures) — данная библиотека основана на библиотеке LAPACK (Linear Algrbra PACKage), расширенной для использования в разнородных системах, функционально идентична базовой по функционированию интерфейса и хранению данных. Задумывалась как простой в использовании порт библиотеки LAPACK с учетом преимуществ GPU имногоядерных архитектур.

PyCuda — открытый проект, реализующий все возможности CUDA с использованием Python. Имеется управление памятью и распределение ресурсов. Также имеется возможность интеграции с NUMPY, набором библиотек для научных вычислений с использованием Python. В качестве отличительной особенности можно указать то, что CUDA программы представляются в виде строковых переменных языка Python, что позволяет использовать некоторые

дополнительные возможности: метаморфизм — изменение исходного кода на лету, полную предобработку кода.

Trust – Deep Dive — стандартная библиотека шаблонов для CUDA, разработанная в nVidia Research. Является проектом с открытым исходным кодом. Данная библиотека использует API CUDA. Для повышения эффективности работы широко используются шаблоны C++. Данная библиотека имитирует стандартную библиотеку шаблонов (STL) и предлагает ряд дополнительных шаблонных алгоритмов и контейнеров.

Библиотекой поддерживается шаблонное метапрограммирование: поддержка встроенных, либо заданных пользователем типов, изменение алгоритмов в соответствии с оперируемым типом данных, переопределение операций. Имеются специализированные и оптимизированные алгоритмы поиска, сортировки, генерации псевдослучайных чисел и др. Данная библиотека по сути выступает в качестве прослойки между самим хостом и устройством GPU.

1.1. Архитектура CUDA

Отличительной особенностью модели параллеллизма, используемой в CUDA, является использование сотен ядер и тысяч параллельных потоков и совместное использование cpu и gpu, не смотря на то, что они являются различными устройствами с раздельной памятью. В действительности происходит разделение на хост(cpu) и устройство(gpu). Хост контролирует процесс выполнения в целом, а устройство выполняет роль высокопроизводительного сопроцессора. При этом функции работы с ядром CUDA вызываются cpu, а фактически выполняются на графическом ускорителе.

Принцип работы самого графического ускорителя возможно описать следующим образом: каждое устройство gpu имеет множество вычислительных ядер, каждое из которых выполняет свой собственный блок потоков. Программа, использующая CUDA, автоматически масштабируется для использования доступной конфигурации ядер с максимальной эффективностью, т. е. CUDA обладает расширяемой моделью для программирования параллельных задач.

Параллельная модель программирования CUDA использует 3-и базовые абстракции:

- иерархия групп потоков,
- разделяемая память,
- барьерная синхронизация.

Эти абстракции обеспечивают параллелизм данных и потоков и позволяют разбивать задачи на отдельные части, которые могут быть выполнены независимыми друг от друга блоками потоков.

Каждая выделенная подпроблема решается совместно и параллельно отдельными потоками в соответствующем блоке. Подобная реализация, с одной стороны, сохраняет выразительность конечного языка разработки, позволяя потокам совместно решать некоторую подзадачу, а с другой стороны, автоматически

увеличивает расширяемость программной платформы, т. к. каждый блок может быть размещен на любых доступных процессорных ядрах, в любой последовательности, как последовательно, так и параллельно, единственное, что нужно знать системе при этом, — это необходимое количество ядер.

Основным языком разработки для платформы CUDA является CUDA C — расширение языка C. Это расширение позволяет разработчику определять специальные функции, называемые ядрами, которые будут вызваны требуемое количество раз, выполняясь параллельно в некотором количестве потоков. Каждый поток, выполняемый ядром, получает уникальный идентификатор, доступный через встроенный объект threadIdx — трёхмерный вектор. Соответственно, потоки могут идентифицироваться им как одно, двух или трёх мерными по формируемым ими пространствам, что позволяет использовать их естественным образом формируя одно, двух либо трёхмерные блоки для соответствующей структуры вычислений (векторы, матрицы и др.). Существует ограничение, налагаемое на количество потоков в одном блоке, т. к. все потоки одного блока выполняются на одном процессорном ядре и должны разделять ограниченные ресурсы ядра. Для существующих на данный момент GPU оно равно 1024.

Так как программное ядро может быть запущенно одновременно в виде нескольких эквивалентных блоков, то общее число потоков определяется как количество блоков, умноженное на количество потоков в блоке. Потоки в блоках организуются в одно или двухмерные системы (сети). Количество блоков в сети определяется размерами данных, которые необходимо обработать, либо количеством процессоров в системе. При запуске ядра задаётся количество блоков в сетке и количество потоков в блоке.

Каждый блок в сетке обладает, в зависимости от конфигурации, одно либо двухмерным идентификатором blockIdx, размерность определяется встроенной переменной blockDim.

Блоки должны иметь возможность использоваться независимо друг от друга в любом порядке как последовательно, так и параллельно, что позволяет создавать программы, автоматически расширяющиеся с увеличением количества ядер в системе. Потоки внутри блока могут взаимодействовать друг с другом через разделяемую память и синхронизировать своё выполнение для координации доступа к памяти.

Потоки могут получать доступ к данным из нескольких пространств памяти. Каждый поток имеет доступ к разделяемой памяти блока, доступной всем потокам, находящимся в одном блоке. Также есть два дополнительных пространства памяти, доступных всем потокам: пространство констант и текстурная память. Эти пространства оптимизированы для использования в различных задачах и имеют различные цели. Текстурная память имеет отличающуюся систему адресации, а также невозможность размещения данных некоторых типов. Глобальная память является общей для всего приложения.

Написание программ для CUDA подразумевает использование одного из двух интерфейсов: CUDA C или CUDA driver API. CUDA C является моделью программирования, использующей расширение языка C. Исходный код, написанный на CUDA C, должен быть скомпилирован при помощи специали-

зированного компилятора (nvcc). Введённые расширения позволяют определять вычислительное ядро как функцию C. При этом задается требуемое количество измерений, блоков и сеток.

CUDA API — это низкоуровневый API на языке C, предоставляющий функции для загрузки ядер в воде готовых сборок и ассемблерного кода для их параллельного исполнения.

CUDA C предоставляет также API времени исполнения. Оба вида API (runtime и driver) предоставляют возможности для управления памятью, предачи данных между памятью хоста и устройства, функции управления системой с несколькими устройствами. Использование runtime API позволяет вести разработку значительно быстрее, в то время как использование driver.api позволяет получить больший уровень контроля, хотя и требует написания большего количества кода и усложняет отладку.

Ядро может быть написано согласно набору инструкций PTX. Результатом компиляции может быть как ассемблерный код (PTX код), так и бинарный объект. При чем для хоста и устройства код генерируется отдельно, но в дальнейшем код устройства может быть привязан к коду хоста в виде глобального массива данных либо запущен самостоятельно на устройстве.

Компилятор обладает функциональностью для обеспечения соответствия итогового кода версии устройства и PTX инструкций, а также задавать минимально допустимые версии устройств и наборов инструкций. Среда выполнения CUDA инициализируется при первом обращении к функциям CUDA. Как только среда инициализировалась в потоке хоста, любые ресурсы, размещённые посредством среды, становятся доступны только в её контексте, при этом поток хоста имеет возможность вызывать только функции среды для оперирования размещёнными ресурсами. Происходит это из-за того, что контекст CUDA, создаваемый при инициализации, доступен только в конкретном потоке хоста и ни в каком другом. В общем случае в системе с несколькими устройствами ядра запускаются на устройстве с индексом 0.

Как было ранее указано, программная модель CUDA представляет собою композицию хоста и устройства, каждый из которых имеет собственную память, при чем вычислительные ядра могут оперировать только с памятью устройства. Память устройства может быть представлена как в виде линейной памяти, так и в виде массива CUDA (данное размещение изначально предназначено и оптимизировано для текстурной выборки).

Линейная память представляет собою 32-х битное адресное пространство для устройств первого поколения (1.x) и 40-а битное для устройств второго поколения (2.x). Также нужно отметить, что данные можно размещать в виде отдельных сущностей, которые могут ссылаться друг на друга через указатели. Для работы с 2-х и 3-х мерными массивами возможно использовать специально оптимизированные функции.

Несколько потоков хоста могут выполнять код на одном и томже устройстве, но предполагается, что один поток хоста может исполняться только на одном устройстве в каждый момент времени.

CUDA поддерживает набор средств для работы с текстурами, используемы-

ми GPU в графических операциях. Чтение данных из текстурной памяти может дать некоторый прирост производительности. Ссылки на текстуры представляют собою ссылки на некоторую область памяти. На одну и туже текстуру может быть назначено несколько ссылок. Элементы текстуры называются текселеми. Текстура может быть представлена любой областью линейной памяти, либо массивом CUDA. Массив CUDA — это размещение памяти оптимизированное для использования текстур, может быть одно, 2-х и 3-х мерным и состоять из 1-го, 2-х, 4-х компонентов на каждый элемент. Каждый компонент может быть знаковым либо беззнаковым 8-и, 16-и или 32-х битным целым, либо 16-и или 32-х битным числом с плавающей точкой единичной точности.

Массивы CUDA читаемы только ядрами посредством выбора текстуры и могут быть только привязаны к текстурам с соответствующей структурой компонентов.

Имеется возможность асинхронно производить следующие операции:

- запуск ядер,
- копирование памяти между устройством и хостом,
- выполнять специализированные функции (помечены префиксом Asynk),
- вызовы функций установки памяти.

Контекст CUDA во многом аналогичен процессу CPU. Все ресурсы и действия обрабатываются в рамках driver API и инкапсулируются внутри контекста CUDA. Система автоматически очищает все занимаемые ресурсы при уничтожении контекста. Каждый контекст обладает собственным 32-х битным адресным пространством, соответственно, данные из разных контекстов ссылаются на различные области памяти. Поток хоста может взаимодействовать только с одним контекстом одновременно, как только контекст создан, он становится текущим для потока.

Вычисления могут проводиться в соответствии с несколькими моделями:

- Default — устройство может быть использовано множеством потоков хоста,
- Exclusive — устройство может использоваться только одним потоком хоста,
- Prohibited — потоки хоста не могут использовать устройство.

Архитектура CUDA построена вокруг расширяемого массива многопоточных Streaming мультипроцессоров. Когда CUDA программа на центральном процессоре хоста запускает на выполнение набор ядер, блоки её составляющие передаются на выполнение доступному количеству процессоров. Все потоки в одном блоке выполняются параллельно на одном процессоре, также несколько блоков могут быть запущены на одном и том же мультипроцессоре. Как только один блок завершает своё выполнение, запускается другой.

Мультипроцессоры созданы таким образом, чтобы выполнять сотни потоков одновременно. Управление этими потоками и их выполнение происходит в соответствии с принципом вычислений SIMT (Single Instruction Multiple Thread). Для максимизации загрузки реализуется параллелизм уровня потоков и параллелизм инструкций в рамках одного потока. Мультипроцессор создаёт и управляет выполнением группами потоков по 32 параллельных потока в каждой. Такие группы называются «основами» (wraps). Отдельные потоки внутри основы стартуют с одного и того же адреса инструкции, но имеют собственные счётчики адреса инструкции, собственные состояния регистров и имеют возможность ветвиться и выполняться независимо друг от друга.

Когда мультипроцессору передают один либо более блоков потоков на выполнение, он разделяется на основы, которые распределяются на выполнение планировщиком основ. Блоки разделяются всегда одним и темже способом. В каждой основе потоки расположены последовательно, с последовательно увеличивающимся идентификатором, при чем первый поток имеет идентификатор равный нулю. Основа выполняет только одну инструкцию одновременно, соответственно, максимальная производительность достигается, когда все 32-а потока в основы совместно перемещаются по инструкциям на выполнение. Если потоки в основе расходятся на зависящие от данных ветви, основа последовательно выполняет каждую ветвь, при этом потоки, не входящие в данную ветвь, находятся в неактивном состоянии. Когда все ветви завершены, потоки объединяются в единый путь выполнения. Разделение на ветви происходит только внутри основы, различные основы выполняются независимо, не смотря на то, выполняют они одни и те же или различные части кода.

Архитектура SIMT сходна с SIMD — векторной организацией, при которой одна инструкция контролирует несколько обрабатывающих элементов. Ключевое отличие в том, что векторная организация SIMD переносит свою структуру и на программное обеспечение, в то время как SIMT инструкции определяют выполнение и поведение ветвления отдельного потока. В противоположность SIMD векторным машинам, SIMT позволяет создавать параллельный код уровня потоков для независимых скалярных потоков также, как и параллельный по данным код для связанных потоков. Программа может даже игнорировать SIMT поведение, если этого требует правильность реализации.

Как бы то ни было значительный прирост скорости возможен только при учёте того, что код должен очень редко требовать от потоков в основе разделяться. Векторные архитектуры в тоже время требуют, чтобы программное обеспечение сливало данные в векторы и самостоятельно обрабатывало ответвления от основного ствола выполнения.

Если неатомарная инструкция, выполняемая основой, пишет в тоже место разделяемой памяти, количество записей произведённое в эту область памяти зависит от вычислительной способности устройства. То какой поток будет последним записавшим, неизвестно. Если атомарная инструкция читает, пишет в одну и ту же локацию глобальной памяти для более чем одного потока, каждое действие для данной локации будет произведено и все они будут сохранены, но порядок, в котором это произойдёт, неизвестен.

1.2. Многопоточность аппаратного обеспечения

Контекст выполнения для каждой основы обрабатывается отдельным мультипроцессором полностью аппаратно на всем протяжении времени жизни основы. Переключение с одного контекста на другой не имеет накладных расходов, т.к. планировщик основ выбирает основы, все потоки которых полностью готовы к выполнению (являются активными) и выполняет следующую инструкцию уже для них каждый из мультипроцессоров имеет набор из 32-х регистров, которые распределены между основами, и параллельный кэш данных/разделяемую память.

Число блоков и основ, которое может быть размещено и обработано вместе на мультипроцессоре для данного ядра зависит от количества регистров и разделяемой памяти, доступной мультипроцессору. Также существует максимальное количество размещаемых блоков и основ для мультипроцессора. Эти ограничения совместно с количеством регистров и разделяемой памяти, доступной мультипроцессору, — являются основой для определения вычислительной способности устройства. В случае, если недостаточно регистров или разделяемой памяти, доступной для мультипроцессора для обработки хотя бы одного блока, ядро не сможет запуститься. Общее количество основ в блоке возможно вычислить по формуле

$$W_{block} = \text{ceil}\left(\frac{T}{W_{size}}, 1\right),$$

где T — число потоков на блок, W_{size} — размер основы (равен 32). Результатом является значение, округлённое к ближайшему целому.

Общее число регистров, доступное в блоке для устройств версии 1.x

$$R_{block} = \text{ceil}(\text{ceil}(W_{block}, G_W) \times W_{size} \times R_k, G_t),$$

для устройств версии 2.x

$$R_{block} = \text{ceil}(R_k \times W_{size}, G_t) \times W_{block},$$

где G_w — гранулярность основы (равна 2), R_k — число регистров для использования ядром, G_t — гранулярность размещения потоков (для устройств версий 1.0 и 1.1 равна 256, для устройств версий 1.2, 1.3 равна 512, для устройств версии 2.0 равна 64), W_{size} — размер основы (равен 32).

Количество размещаемой памяти на блок:

$$S_{block} = \text{ceil}(R_k, G_s),$$

S_k — количество используемой разделяемой памяти в байтах, G_s — гранулярность размещения памяти (512 для моделей 1.x, 128 для моделей 2.0).

В системах с несколькими графическими ускорителями все поддерживающие технологию устройства доступны при помощи драйвера по отдельности.

2. OpenCl

Open CL (Open Computing Language) — открытый api для вычислений в гетерогенной среде. Предоставляет единообразную среду программирования для разработки переносимого кода, использующего разнородную смесь из многоядерных CPU, GPU, процессоров архитектуры Cell и других параллельных процессоров, как DSP.

Процессоры CELL — это совместная разработка компаний Sony, IBM и Toshiba, ориентированная, в основном, на мультимедийные приложения. Процессор состоит из центрального процессора общего назначения (PowerPC), называемого PPE, и восьми процессоров специального назначения (SPE), доступных исключительно для численных вычислений. Каждый SPE может выполнять векторные операции, которые может выполнять на множестве наборов данных для каждой инструкции. По причине гетерогенного принципа построения CELL процессор значительно отличается от традиционных мультипроцессоров. Результатом такого дизайна является то, что один CELL процессор с частотой 3,2 ГГц может достигнуть пиковой производительности более 200 GFLOP/сек в вычислениях с плавающей точкой одинарной точности и до 15 GFLOP/сек для двойной точности (до 100 GFLOP/сек при использовании более современного PowerXCell процессора). Но при этом разработчикам программного обеспечения для данного типа процессоров требуется вручную управлять передачей данных между SPE и PPE.

Стандарт OpenCL во многом похож на платформу CUDA от nVidia, но данный стандарт существенно отличается по кругу систем, к которым он применим. CUDA разрабатывался исключительно для использования с GPU устройствами nVidia, в то время как Open CL должен поддерживать значительно более широкий круг устройств.

Стандарт состоит из API для координации параллельных вычислений в среде разнородных процессоров и кроссплатформенного языка программирования с хорошо специфицированной вычислительной средой. Стандарт поддерживает как программную модель параллелизма данных, так и задач. В качестве базового языка программирования используется разновидность ISO C99 с расширением для поддержки параллелизма. Численные типы данных, используемые стандартом, соответствуют стандарту IEEE 754. В рамках стандарта определены конфигурационные профили для портативных и встраиваемых устройств. Также определены правила взаимодействия с OpenGL, OpenGL ES и другими графическими API.

Сама спецификация разделена на три части: базовая спецификация, которую должен поддерживать каждый OpenCL компилятор, профили для портативных и сменных устройств, позволяющие использовать подобные устройства, учитывая их технологические особенности, и набор опциональных расширений, которые планируется добавить в базовую спецификацию в следующих ревизиях стандарта. Платформа, основанная на этих разработанных спецификациях, включает в себя язык программирования, API, библиотеки и среду выполнения.

2.1. Архитектура OpenCL

Модель платформы представляет собою хост, соединённый с одним либо несколькими OpenCL устройствами. Каждое устройство разделяется на один либо более вычислительных элементов, на которых и производятся все вычисления. Приложение OpenCL выполняется на хосте соответственно родной для данного хоста модели. Приложение вызывает команды с хоста для выполнения вычислений на устройстве. Каждый вычислительный элемент выполняет один поток инструкций как SIMD или SPMD устройство(где каждый PE имеет собственный счётчик инструкций).

OpenCL разработан для поддержки устройств с различными вычислительными возможностями в рамках единой платформы. Что включает устройства, поддерживаемые различными версиями спецификаций. Основными показателями являются: версия платформы, версия устройства и версия языка OpenCL C, поддерживаемая устройством.

Выполнение любой OpenCL программы состоит из двух частей: ядер, выполняемых на одном или нескольких устройствах, и программы хоста. Программа хоста определяет контекст ядер и управляет их выполнением. Когда ядро утверждается на выполнение, определяется индексное пространство. Экземпляр ядра выполняется для каждой точки из этого пространства. Такой экземпляр ядра называется рабочим элементом и определяется своими координатами в индексном пространстве — глобальным идентификатором рабочего элемента. Каждый рабочий элемент выполняет тот же код, за исключением специфических путей выполнения и различия данных между конкретными рабочими элементами.

Индексное пространство, поддерживаемое OpenCL, называется NDRage. NDRange — это N-мерное индексное пространство с размерностью, равной одному, двум или трём. Глобальный и локальный идентификаторы рабочего элемента являются N-мерными кортежами. Рабочим группам идентификаторы присваиваются сходным с глобальными идентификаторами образом. Рабочие элементы, назначенные в рабочие группы, получают локальный идентификатор из диапазона от нуля до размера рабочей группы в данном измерении минус один. Комбинация идентификатора группы и локального идентификатора рабочего элемента однозначно определяет рабочий элемент. Каждый рабочий элемент определяем двумя путями: с помощью глобального идентификатора или с помощью комбинации идентификатора группы и локального идентификатора внутри данной рабочей группы.

На подобную программную модель возможно отобразить большое количество программных моделей. OpenCL явно поддерживает две модели: параллелизм данных и параллелизм задач.

Контекст Выполнения ядра определяется хостом, при этом контекст включает в себя такие ресурсы как:

- устройства: коллекция OpenCL устройств доступных для использования хостом,
- ядра: функции OpenCL, запускаемые на OpenCL устройствах,

- программные объекты: программные коды, реализующие ядра,
- объекты памяти: набор объектов памяти, видимых хосту и устройствам. Объекты памяти содержат данные, над которыми могут провести операции экземпляры ядер.

Контекст создаётся и управляется устройством посредством функций, предоставляемых OpenCL API. Хост создаёт структуру данных, называемую «очередью команд», для координации выполнения программных ядер на устройствах. Хост помещает команды в командную очередь, которые затем планируются для конкретного устройства в контексте.

Команды включают в себя:

- команды выполнения ядра: запуск ядра на вычислительных элементах устройства,
- команды памяти: передача данных как между хостом и объектами памяти, так и между ними самими, включает отображение объектов памяти как на адресное пространство хоста, так и из него,
- команды синхронизации: определяют порядок выполнения команд.

Очередь команд планирует выполнение команд на устройстве. Команды могут выполняться относительно друг друга в одном из двух вариантах:

- по порядку: команды запускаются в порядке своего добавления в очередь выполнения и начинают выполняться после завершения предыдущей,
- беспорядочно: команды запускаются по порядку, но не ожидают завершения предыдущей команды перед собственным запуском.

Модель выполнения OpenCL поддерживает два типа ядер.

Ядра OpenCL, написанные при помощи языка программирования OpenCL C и скомпилированные соответствующим компилятором. Каждая реализация OpenCL поддерживает такие ядра.

Ядра, написанные для конкретных платформ (native), доступные через указатель на функцию хоста. Такие ядра выполняются последовательно, как и ядра OpenCL, и разделяют с ними объекты памяти. Родными объектами могут быть ядра определённые, как функция в коде приложения или экспортированы из библиотеки. Возможность запускать такие ядра является функциональной и зависит от конкретного устройства и реализации ядра. Тем не менее в API OpenCL включены функции для проверки возможности запуска ядра на конкретном устройстве.

Рабочие элементы, выполняющие ядро, имеют доступ к четырём различным областям памяти:

- глобальная память — область памяти, доступ как на чтение, так и на запись в которую имеют все рабочие элементы всех групп, при этом обращения к этой области памяти у некоторых устройств могут кэшироваться,

Таблица 1. Размещение данных и доступ к различным видам памяти

	Глобальная	Констант	Локальная	Частная
Хост	Динамическое размещение Доступ на чтение и запись	Динамическое размещение Доступ на чтение и запись	Динамическое размещение Нет доступа	Нет возможности размещения Нет доступа
Ядро	Нет возможности размещения Доступ на чтение и запись	Статическое размещение Доступ только на чтение	Статическое размещение Доступ на чтение и запись	Статическое размещение Доступ на чтение и запись

- область памяти констант — область глобальной памяти, содержащая константы во время выполнения ядра (данные внутри этого объекта размещаются и инициализируются хостом),
- локальная память — область памяти рабочей группы, может использоваться для размещения переменных и данных, разделяемых всеми рабочими элементами группы (реализацией этой области может быть как выделенная область памяти, так и отображение на некоторую часть глобальной памяти),
- частная память — область памяти, используемая непосредственно некоторым рабочим элементом (данные, размещённые в этой области, невидимы нигде за её пределами).

В таблице 1 описаны возможности записи в различные области памяти для хоста и устройства.

Приложение, запущенное на хосте, использует API для создания объектов в глобальной памяти и управления ими. По большей части хост и память устройства независимы друг от друга. Так как устройство определяется вне OpenCL, но хосту необходимо с ним взаимодействовать, то приходится это делать одним из двух способов: явным копированием областей памяти от устройства к хосту и наоборот, и отображением участков памяти и объектов.

Для копирования данных устройством выполняется команда передачи данных между объектом памяти и памятью хоста. При чем команды передачи могут быть как блокирующими, так и неблокирующими. Блокирующая передача возвращает данные, как только ими можно будет безопасно пользоваться, неблокирующая возвращает данные непосредственно после запуска вне зависимости от безопасности их использования.

Методы отображения позволяют хосту отразить некоторую область объекта памяти в своё адресное пространство. Эти команды также могут быть блокирующими или неблокирующими. Как только некоторая область памяти была связана с хостом, он может свободно писать в неё, либо читать из неё. Хост отвязывает область памяти, как только его взаимодействие с ней завершилось. OpenCL использует слабосвязную модель памяти, т. е. не гарантируется, что

состояние объекта, видимое некоторым рабочим элементом, все время совпадает с состоянием, видимым любым другим рабочим элементом.

OpenCL поддерживает модели параллельности данных и задач, основной является модель параллельности данных. Параллелизм данных определяет вычисления как последовательность инструкций, применяемую на множество объектов в памяти. Индексное пространство, связанное с моделью выполнения OpenCL, определяет рабочие элементы и то, как данные связываются с ними. В структурированной модели параллелизма данных существует однозначное соответствие между рабочими элементами и данными, направленными на параллельную обработку. OpenCL реализует облегчённую модель параллелизма данных, при котором не требуется соответствия один к одному. Предоставляется иерархическая модель параллелизма данных. Существует две возможности определения иерархического подразделения данных. В случае явной модели программист определяет общее количество вычислительных элементов, которые должны быть запущены параллельно, а также то, как они будут распределены среди рабочих групп. В неявной модели программист определяет только общее количество рабочих элементов на запуск, а их разделение на группы управляется средой OpenCL. Параллелизм задач определяет модель, в которой любой экземпляр ядра выполняется вне зависимости от какого бы то ни было индексного пространства. Логически это соответствует выполнению ядра на вычислительном узле с рабочей группой, содержащей только один рабочий элемент. В данной модели параллелизм выражается:

- использованием векторных типов данных, реализуемых устройством,
- выполнением нескольких задач,
- выполнением родных ядер с использованием программной модели ортогональной к OpenCL.

2.2. Синхронизация в OpenCL

В OpenCL существует два домена синхронизации:

- среди рабочих элементов в общей рабочей группе,
- команды, запущенные в одном контексте выполнения.

Синхронизация в пределах одной рабочей группы реализуется при помощи барьеров рабочей группы. Все рабочие элементы рабочей группы должны выполнить барьер, прежде чем они смогут выполнять инструкции за ним. Нужно отметить, что не предусмотрено возможностей синхронизации между рабочими группами.

Синхронизационными точками между командами в очереди команд являются: барьеры командной очереди гарантируют, что все ранее выполнявшиеся команды завершены и результаты произведённых ими изменений видны последующим командам до начала их выполнения. Этот тип может быть использован

только для синхронизации между командами в последовательной очереди команд.

Ожидание события завершения выполнения команды — это событие генерируется каждой командой после того, как выполнение завершено и состояние данных обновлено. Следующая команда ожидает появления этого события, после чего запускается сама.

3. Сравнение быстродействия программ, использующих платформы CUDA и OpenCL

Ядра OpenCL в отличие от ядер CUDA могут быть скомпилированы во время выполнения программы. С одной стороны, эта компиляция «на лету» позволяет генерировать код, оптимизированный для конкретного целевого устройства, но при этом на саму компиляцию тратится дополнительное время. В тоже время CUDA разработана непосредственно производителем аппаратного обеспечения и в ней учитываются все особенности продукции, при этом архитектура программной системы тесно связана с аппаратной архитектурой. Это позволяет добиваться большей оптимизации итогового кода. Тем не менее программная архитектура систем практически идентична, и, в случае запуска систем на одном и том же целевом вычислительном устройстве, различия в производительности будут вызваны различиями в программной реализации: оптимизацией драйверов устройства, уровнем оптимизации кода компилятором.

Для проверки выбираются алгоритмы, наиболее легко ложащиеся на обе платформы. Процесс вычислений организуется таким образом, чтобы максимально загрузить видеокарту. Для этого прибегают к минимальному взаимодействию ядра с центральным процессором во время вычислений, минимизируют передачу данных и передаваемые объёмы данных.

В работе [2] для проведения проверки используется адиабатический квантовый алгоритм, написанный на C++. Оригинальное ядро было разработано для CUDA и далее модифицировалось для использования в OpenCL таким образом, чтобы минимизировать вносимые изменения.

Общие результаты выполнения приведены в таблице 2. Совокупность результатов, полученных авторами, показывает, что CUDA лучше справляется с передачей данных между хостом и графической картой, также реализация CUDA быстрее справляется со своей задачей, чем аналогичная реализация с использованием OpenCL. Различия в производительности по результатам измерений составляют примерно 10-20% (хотя отставание в производительности ядра может превышать и 60%), что позволяет авторам говорить о большей пригодности CUDA для высоконагруженных приложений, но при этом универсальность OpenCL позволяет использовать большее количество целевых устройств.

В таблице 2 stdev — среднеквадратичное отклонение результатов измерений.

В тоже время нужно отметить, что даже при некотором отставании в скорости вычислений от CUDA OpenCL выигрывает тем, что предоставляет возможности переносимости без потерь в вычислительных возможностях приложения.

Таблица 2. Сравнительные результаты работы программы

Кубиты	Время выполнения на GPU				Общее время выполнения			
	OpenCL		CUDA		OpenCL		CUDA	
	среднее	stdev	среднее	stdev	среднее	stdev	среднее	stdev
8	1,97	0,027	2,23	0,004	2,94	0,007	4,28	0,164
16	3,87	0,006	4,73	0,013	5,39	0,008	7,45	0,023
32	7,71	0,007	9,01	0,010	10,16	0,009	12,84	0,006
48	13,75	0,015	19,81	0,085	17,75	0,013	26,69	0,016
72	26,04	0,036	42,17	0,062	23,77	0,025	54,85	0,103
96	61,32	0,065	71,99	0,055	76,24	0,033	92,97	0,064
128	101,07	0,527	113,54	0,758	123,54	1,091	142,97	1,080

Сравнительные результаты вычислений при оптимизации под различные платформы приведены в работах [3, 4].

Литература

1. Tesla C2050 performance bench mark. URL: `http://www.microway.com/pdfs/TeslaC2050-Fermi-Performance.pdf` (дата обращения: 7.11.2011).
2. Karimi K., Dickson N.G., Hamze F. A Performance Comparison of CUDA and OpenCL. URL: `http://ru.arxiv.org/abs/1005.2581v3` (дата обращения: 15.09.2011).
3. Khannaa G., McKennonb J. Numerical modeling of gravitational wave sources accelerated by OpenCL. URL: `http://arxiv.org/abs/1001.3631` (дата обращения: 7.10.2011).
4. Pang B., Pen U., Perrone M. Magnetohydrodynamics on Heterogenous architectures: a perfomance comparison. URL: `http://arxiv.org/abs/1004.1680` (дата обращения: 11.09.2011).

Математические структуры и моделирование
2012, вып. 26, с. 89–93

УДК 519.16:004.372.2

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ОПРЕДЕЛЕНИЯ ИЗОМОРФНОСТИ ГРАФОВ В СИСТЕМАХ С РАСПРЕДЕЛЁННОЙ И ОБЩЕЙ ПАМЯТЬЮ

Д.Э. Вильховский, С.С. Ефимов

Задача проверки изоморфности графов часто возникает в химии, экономике, статистике, теоретической физике, математической лингвистике и других областях. Целью проведённого исследования являлся сравнительный анализ эффективности использования инвариантов и параллельных реализаций алгоритмов проверки изоморфности графов.

1. Методы определения изоморфности графов

Для определения изоморфности графов используется два основных подхода. В первом выполняется попытка перебора всех возможных перестановок. При наличии у разных графов совпадающих перестановок считается, что графы изоморфны. Недостатки этого подхода очевидны: из-за необходимости перебора всех n! перестановок, при некотором значении n необходимое для вычисления время делает эту задачу нерешаемой в реальном масштабе времени. При втором подходе пытаются найти такой инвариант, из совпадения которого следовало бы, что графы изоморфны. К недостаткам этого подхода стоит отнести тот факт [1, с.193], что не существует полного инварианта, вычислимого за полиномиальное время.

1.1. Список основных инвариантов

Среди наиболее распространённых инвариантов решения задачи определения изоморфизма графов можно назвать следующие:

- индекс Винера,
- определитель матрицы смежности,
- число вершин и число дуг/рёбер,
- индекс Рандича,

Copyright © 2012 **Д.Э. Вильховский, С.С. Ефимов**
Омский государственный университет им. Ф.М. Достоевского
E-mail: vilkhovskiy@gmail.com, s_efimov@mail.ru

- диаметр графа,
- индекс Хосойи,
- минимальное число вершин, необходимое для покрытия рёбер,
- упорядоченный по возрастанию или убыванию вектор собственных чисел матрицы смежности графа (спектр графа),
- характеристический многочлен матрицы смежности,
- упорядоченный по возрастанию или убыванию вектор собственных чисел матрицы смежности графа (спектр графа),
- характеристический многочлен матрицы смежности.

1.2. Описание инвариантов

В данной работе были рассмотрены следующие инварианты:

Число вершин и число дуг/рёбер. Для вычисления необходимо сверить число вершин с различными степенями

Индекс Винера — величина $w{=}\sum\limits_{\forall i,j} d(v_i, v_j)$, где $d(v_i, v_j)$ минимальное расстояние между вершинами v_i, v_j.

Индекс Рандича — величина $r = \sum\limits_{(v_i,v_j)\in V} \dfrac{1}{\sqrt{d(v_i) * d(v_j)}}$, где $d(v_i), d(v_j)$ степени вершин v_i, v_j соответственно.

1.3. Описание прямого алгоритма проверки изоморфности графов

Для распараллеливания задачи был написан метод, который позволяет определить итоговую перестановку по её номеру. В результате, каждая вычислительная машина в кластере получала для обработки свой диапазон значений. Далее результаты проверки отправлялись корневому процессу, который собирал результаты и анализировал их.

Проверка эффективности параллельной реализации прямого алгоритма исследовалась на следующих классах графов:

- планарный граф,
- дерево,
- двудольный граф.

2. Реализация алгоритмов

Для проверки эффективности инвариантов генерировались всевозможные неориентированные графы с заданным числом вершин m. По числу найденных изоморфных графов с помощью инварианта можно судить о его эффективности. Если это число совпадает с количеством изоморфных графов, найденных прямым методом, то выполняется достаточность инварианта для всех графов с числом вершин m.

При реализации алгоритмов использовались следующие технические и программные средства.

- Java SE 6 update 31
- MPJ Express v0.38
- 9 персональных компьютеров (кластер невыделенных рабочих станций)
  - ◇ Процессор — Dual-Core E5200 2,5 Ghz;
  - ◇ Память — 3,24 Гб;
  - ◇ Mandriva Linux;
  - ◇ Сеть — 100 Мбит/сек.

3. Результаты экспериментов

Число вершин и число дуг/рёбер

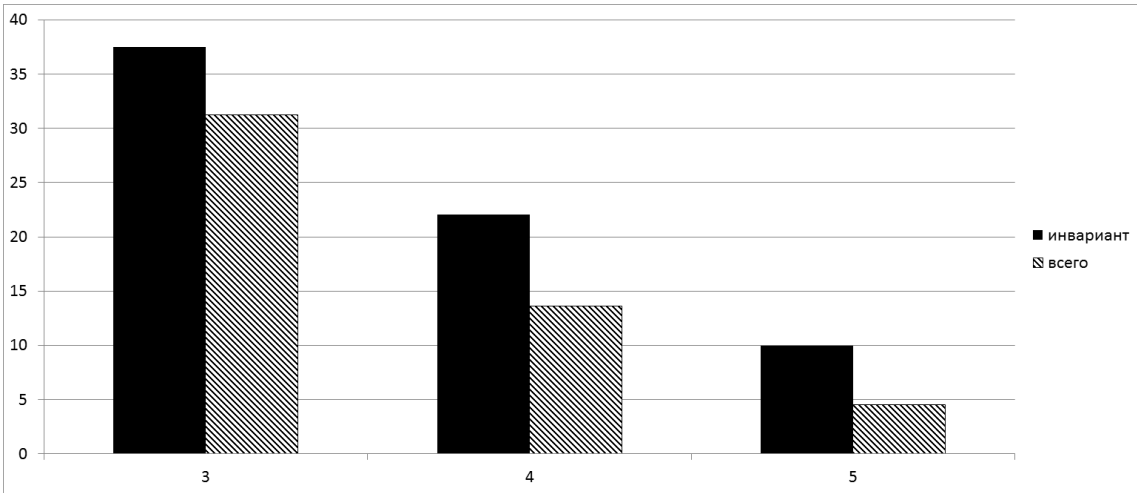

Рис. 1. Процент изоморфных графов, найденных с помощью инварианта «число вершин и число дуг/рёбер»

Из результатов видно, что данный инвариант не даёт достаточности для графов с числом вершин равным трём.

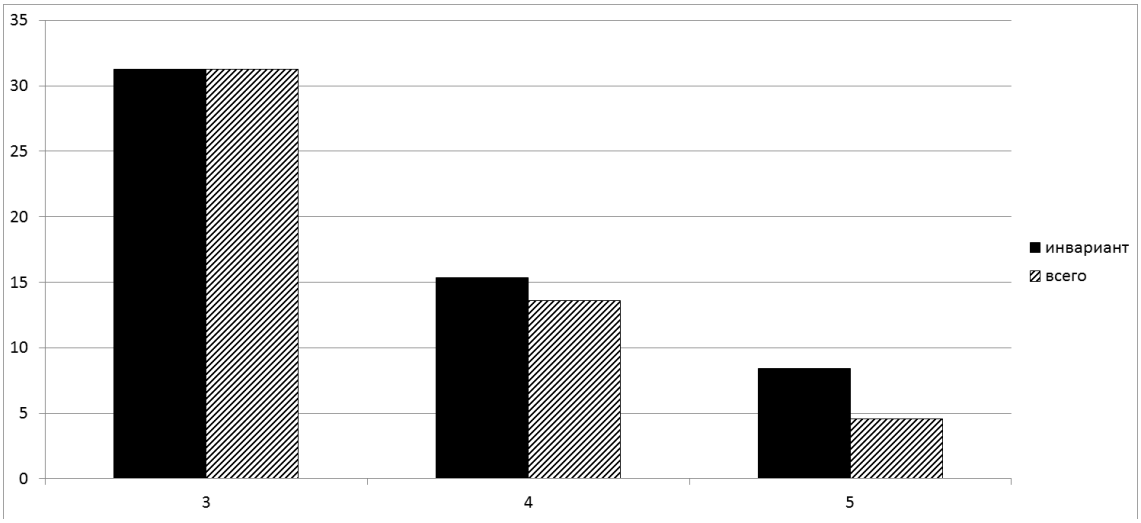

Рис. 2. Процент изоморфных графов, найденных с помощью инварианта Индекс Винера

Индекс Винера

Данный инвариант даёт достаточность для графов с числом вершин, не превосходящим трёх. Однако стоит заметить, что для его вычисления нам необходимо воспользоваться алгоритмом Флойда-Уоршелла, сложность которого составляет $o(n^3)$.

Индекс Рандича

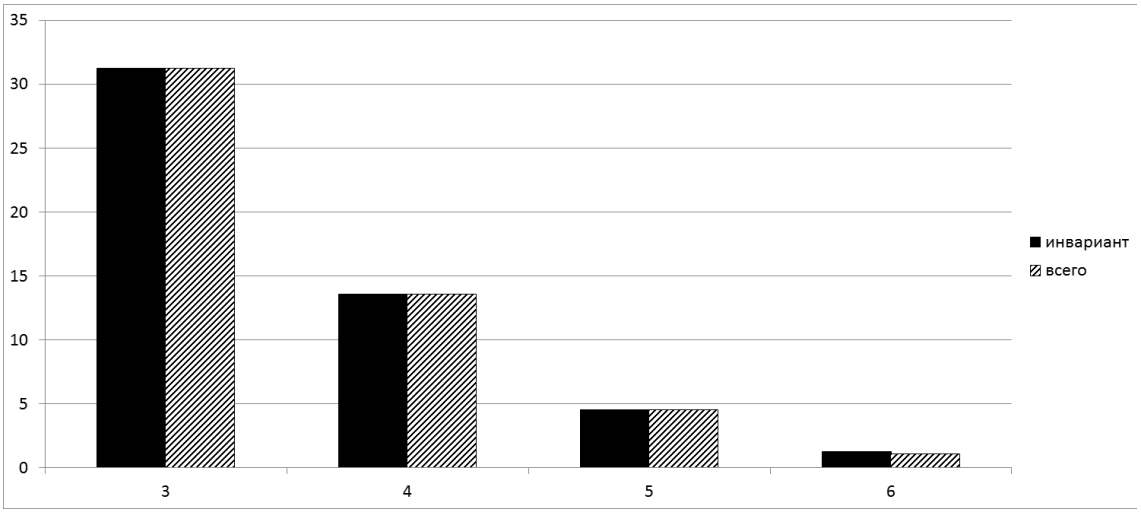

Рис. 3. Процент изоморфных графов, найденных с помощью инварианта Индекс Рандича

Данный инвариант является самым эффективным из всех рассмотренных в этой работе инвариантов. Он даёт достаточное условие для графов с числом вершин, не превосходящих 5.

По результатам анализа данных инвариантов можно сделать вывод, что при рассмотрении графов с числом вершин, превосходящих 5, придётся использовать прямой алгоритм проверки изоморфности графов.

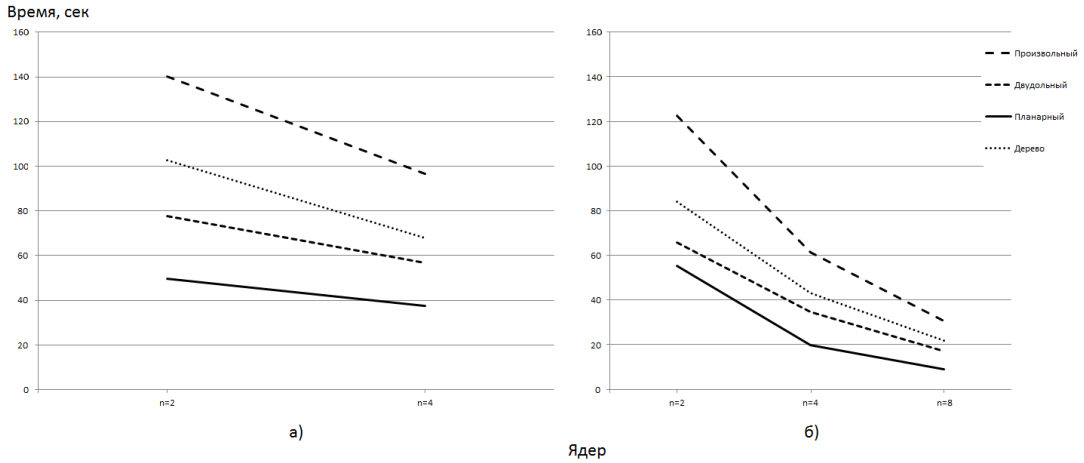

Рис. 4. Зависимость времени от числа ядер: а) распределённая память, б) общая

4. Заключение

В результате проведённых исследований оказалось, что в общем случае самым эффективным инвариантом является индекс Рандича, но его использование имеет смысл только тогда, когда число вершин у графов меньше 5, т.к. при большем количестве вершин условие достаточности не выполняется. Для более сложных графов применялся прямой алгоритм проверки. В результате использования его параллельной реализации в модели с общей памятью было получено небольшое ускорение, что связано с необходимостью частого выделения и освобождения памяти. Параллельная реализация в модели с распределённой памятью показала хорошее линейное ускорение.

Литература

1. Новиков Ф.А. Дискретная математика для программистов. СПБ : Питер, 2000. 304 с.

Математические структуры и моделирование
2012, вып. 26, с. 94–109

УДК 519.688:004.75

ПАРАЛЛЕЛЬНАЯ РЕАЛИЗАЦИЯ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ФАКТОРИЗАЦИИ В СИСТЕМАХ С РАСПРЕДЕЛЁННОЙ ПАМЯТЬЮ

А.В. Макаренко, А.В. Пыхтеев, С.С. Ефимов

В статье рассматриваются наиболее популярные на сегодняшний день алгоритмы факторизации целых чисел, предложена их параллельная реализация в системах с распределённой памятью. Получены сравнительные оценки для каждого метода на различном числе параллельных процессов. Сделаны общие выводы об эффективности использования алгоритмов.

Введение

Некоторые часто используемые алгоритмы асимметричного шифрования, такие как RSA, используют вычислительную сложность факторизации в качестве основы своей криптостойкости. Если для гипотетического квантового компьютера алгоритм, осуществляющий разложение числа на простые множители за полиномиальное время, уже разработан, то вопрос существования такового для классического компьютера остаётся открытым. А значит, ускорение существующих методов факторизации является одной из наиболее актуальных задач. Кроме всевозможных доработок и улучшений самих алгоритмов наиболее эффективным средством ускорения их работы является параллельная реализация и выполнение на системах с распределённой или общей памятью.

Ранее K.A. Kanabar проводил достаточно объёмные исследования некоторых распространённых алгоритмов факторизации, в том числе анализировались такие, как метод Ферма, ρ-метод Полларда, метод эллиптических кривых, которые также были исследованы в настоящей работе. Kanabar предложил такую методику измерений, при которой используются числа с двумя близкими сомножителями, тремя близкими сомножителями или тремя произвольными сомножителями. При этом последовательно увеличивается разрядность исследуемых чисел. В работе также приведены общие результаты по сравнению быстродействия алгоритмов факторизации, среди которых, кроме названных выше, исследовались метод последовательного деления и (P-1)-метод Полларда.

Copyright © 2012 **А.В. Макаренко, А.В. Пыхтеев, С.С. Ефимов**
Омский государственный университет им. Ф.М. Достоевского
E-mail: alv.makarenko@gmail.com, alex.pykhteyev@gmail.com, s_efimov@mail.ru

R.P. Brent в своей работе [1] обобщил способы модификации и улучшения многих алгоритмов факторизации, а также привёл несколько рекомендаций по частичной или полной параллельной реализации алгоритмов, многие из которых были использованы нами в данном исследовании. Также были приведены оценки ускорения работы параллельных алгоритмов по сравнению со своими последовательными аналогами и их строгое математическое обоснование.

Цель проведённого исследования — реализовать параллельные алгоритмы факторизации, оценить их эффективность, сравнив и систематизировав результаты, полученные в ходе проведения экспериментов.

В данной работе использовались алгоритмы и результаты описанные в [1–7].

1. Алгоритмы факторизации

В работе исследованы следующие методы:

Экспоненциальные:

- метод Ферма,
- ρ-метод Полларда,
- метод Лемана,
- метод Шенкса.

Субэкспоненциальные:

- метод эллиптических кривых,
- метод квадратичного решета.

Классификация методов произведена в соответствии с их вычислительной сложностью.

Далее следует псевдокод вышеназванных методов на алгоритмическом языке, составленный нами на основе реального программного кода, а также описаны особенности параллельной реализации алгоритмов.

1.1. Метод Ферма

На входе: нечётное число n

1: $x \leftarrow [\sqrt{n}]$
2: $y \leftarrow x^2 - n$
3: **while** $\mathrm{isSquare}\,(y) \neq$ **true do**
4: $\quad x \leftarrow x + 1$
5: $\quad y \leftarrow x^2 - n$

end while
$s \leftarrow x - \sqrt{y}$
$t \leftarrow x + \sqrt{y}$
if $s \neq 1$ **and** $s \neq n$ **then**
    return s, t
end if

Функция isSquare $(\dots)$ возвращает $true$, если аргумент является полным квадратом, и $false$ иначе.

Параллельная реализация основана на том, что каждый процесс, участвующий в факторизации, обрабатывает свои значения в качестве кандидатов на число x, проверяет все условия, описанные в алгоритме, определяя, найден ли нетривиальный множитель. Через некоторые промежутки времени главный процесс-координатор «опрашивает» вычислительные процессы на предмет выявления множителя. Если этот множитель найден одним из процессов, то поступает сигнал о завершении всех процессов, иначе продолжается поиск множителей.

1.2. Метод Шермана Лемана

На входе: нечётное число n.

for $a \leftarrow 2$ **to** $\left[n^{1/3}\right]$ **do**
    if $a|n$ **then**
        return a
    end if
end for
for $k \leftarrow 1$ **to** $\left[\mathrm{n}^{1/3}\right]$ **do**
    for $d \leftarrow 0$ **to** $\left[\frac{n^{1/6}}{4\sqrt{k}}\right] + 1$ **do**
        if isSquare $\left(\left(\left[\sqrt{4kn}\right] + d\right)^2 - 4kn\right)$=**true then**
            $A \leftarrow \left[\sqrt{4kn}\right] + d$
            $B \leftarrow \sqrt{A^2 - 4kn}$
            if $1 < \gcd(A + B, n) < n$ **then**
                return $A + B$
            else if $1 < \gcd(A - B, n) < n$ **then**
                return $(A - B)$
            end if
        end if
    end for
end for

Функция $\gcd(\dots)$ возвращает наибольший общий делитель аргументов.

Параллельная реализация аналогична таковой в методе Ферма. На первом шаге каждый процесс обрабатывает свои значения числа a, на втором шаге

каждый процесс проверяет свой диапазон чисел k. При этом результаты через некоторое количество итераций отправляются главному процессу-координатору, вследствие чего им принимается решение о завершении всех процессов, если нетривиальный множитель найден, или о продолжении работы алгоритма.

1.3. Метод Шенкса

На входе: нечётное число n, маленький множитель k

$P_0 \leftarrow \left\lceil \sqrt{kn} \right\rceil$
$Q_0 \leftarrow 1$
$Q_1 \leftarrow kn - P_0^2$
repeat
    $b_i \leftarrow \left\lfloor \dfrac{\left\lceil \sqrt{kn} \right\rceil + P_{i-1}}{Q_i} \right\rfloor$
    $P_i \leftarrow b_i Q_i - P_{i-1}$
    $Q_{i+1} \leftarrow Q_{i-1} + b_i \left(P_{i-1} - P_i\right)$
until isSquare$(Q_i) =$ **false**
$b_0 \leftarrow \left\lfloor \dfrac{\left\lceil \sqrt{kn} \right\rceil + P_{i-1}}{Q_i} \right\rfloor$
$P_0 \leftarrow b_0 \sqrt{Q_i} + P_{i-1}$
$Q_0 \leftarrow \sqrt{Q_i}$, $Q_1 \leftarrow \dfrac{kn - P_0^2}{Q_0}$
repeat
    $b_i \leftarrow \left\lfloor \dfrac{\left\lceil \sqrt{kn} \right\rceil + P_{i-1}}{Q_i} \right\rfloor$
    $P_i \leftarrow b_i Q_i - P_{i-1}$
    $Q_{i+1} \leftarrow Q_{i-1} + b_i \left(P_{i-1} - P_i\right)$
until $P_{i-1} \neq P_i$
if $1 < \gcd(P_i, n) < n$ **then**
    return $\gcd(P_i, n)$
end if
return FAIL

Если нетривиальный делитель не найден, то следует использовать другое значение k.

Параллельная реализация данного алгоритма заключается в использовании различных маленьких множителей k. Главный процесс выступает в роли координатора. Остальные процессы выполняют описанный выше алгоритм со своим k. Как только какой-либо из процессов находит нетривиальный делитель, то происходит отправка его координатору, который посылает сигнал завершения работы алгоритма каждому процессу.

1.4. Метод ρ-Полларда

На входе: нечётное число n.

1: $x_i \leftarrow \text{Random}\,(n)$
2: $x_{2i} \leftarrow f\,(x_i) \mod n$
3: **while** $\gcd\,(x_{2i} - x_i, n) = 1$ **or** $\gcd\,(x_{2i} - x_i, n) = n$ **do**
4: $\quad x_i \leftarrow f\,(x_i) \mod n$
5: $\quad x_{2i} \leftarrow f(f\,(x_i)) \mod n$
6: **end while**
7: **return** $\gcd\,(x_{2i} - x_i, n)$

Функция $Random\,(n)$ возвращает случайное число от 1 до n. Функция $f\,(x_i)$ выбирается с коэффициентами из Z_n. Обычно, $f\,(x_i) = x^2 + 1$.

Параллельная реализация данного алгоритма заключается в генерации различных значений x_i для каждого процесса. Главный процесс выступает в роли координатора. Таким образом, удаётся просмотреть различные рекуррентные последовательности для поиска нетривиального делителя. Как только какой-либо из процессов находит нетривиальный делитель, то происходит отправка его координатору, который посылает сигнал завершения работы алгоритма каждому процессу.

1.5. Метод эллиптических кривых

На входе: число n, границы $v\,(n)\,,\ w\,(n) \in\ \mathbb{N}$. Выбираем случайную ЭК $E_{a,b} \mod n$ и точку $P_0 = (x_0, y_0)$ на ней.

1: $k \leftarrow 1$
2: $m \leftarrow 0$
3: **for** r – простое, $r \leftarrow 2$ **to** w **do**
4: $\quad$ **while** $r^m \leq v + 2\sqrt{v} + 1$ **do**
5: $\quad\quad m \leftarrow m + 1$
6: $\quad$ **end while**
7: $\quad k \leftarrow k \times r^m$
8: $\quad m \leftarrow 0$
9: **end for**
10: $d \leftarrow \text{compute}(kP_0)$
11: **if** $1 < d < n$ **then**
12: $\quad$ **return** d
13: **end if**
14: **return** FAIL

Функция compute(kP) возвращает делитель числа n в ходе вычисления кратного k точки P. Возвращаемое значение FAIL в алгоритме означает, что метод эллиптических кривых является вероятностным, и попытка нахождения нетривиального делителя по вышеописанному алгоритму не всегда даёт положительный результат.

Параллельная реализация основана на том, что каждый процесс выбирает разные эллиптические кривые и далее выполняет алгоритм, описанный выше, без изменений.

1.6. Метод квадратичного решета

На входе: число n, количество чисел k факторной базы, радиус интервала просеивания L.

1: $FB \leftarrow$ buildFactorBase(k)
2: **for** $i \leftarrow 1$ **to** k **do**
3: $x \leftarrow$ solveEquation($FB[i]$)
4: solutions.add($x, FB[i]$)
5: **end for**
6: **for** $i \leftarrow -L$ **to** L **do**
7: $W[i] \leftarrow (m+i)^2 - n$
8: **end for**
9: **for** $i \leftarrow 1$ **to** solutions.size() **do**
10: sieving($solutions[i]$)
11: **end for**
12: $M \leftarrow$ createMatrix()
13: **if** $1 <$ solveMatrix(M) $< n$ **then**
14: **return** solveMatrix(M)
15: **end if**
16: **return** FAIL

Функция buildFactorBase(k) возвращает факторную базу размерностью k. Функция solveEquation(FB[i]) ищет решение сравнения:

$$(m+x)^2 - n \equiv 0 \pmod{FB[i]},$$

где $m = [\sqrt{n}]$. Массив solutions хранит пары чисел (x, p), где x является решением сравнения $(m+x)^2 - n \equiv 0 \pmod{p}$. Функция solutions.size() возвращает размер массива solutions. Функция createMatrix() строит систему линейных уравнений. Функция solveMatrix(M) решает систему линейных уравнений и возвращает делитель (возможно тривиальный) числа n.

Если нетривиальный делитель не был получен, то следует увеличить радиус просеивания или размер факторной базы.

Параллельная реализация данного алгоритма заключается в разбиении интервала просеивания на несколько частей. Каждый процесс ищет гладкие числа в своём интервале и результат отправляет главному процессу, который собирает все данные и переходит к составлению системы линейных уравнений на основе полученной информации.

2. Результаты экспериментов

Все алгоритмы выполнялись на языке программирования Java с использованием Java SE 6 update 31. Для параллельной реализации алгоритмов исполь-

зовалась адаптация для Java интерфейса передачи сообщений MPI (Message Passing Interface) — MPJ Express v0.38.

Исследование проводилось на компьютерах следующей конфигурации:

- ЦП — Dual Core E5200 2.5 ГГц,
- ОЗУ — 3.24 Гб,
- ОС — Mandriva Linux 2008,
- ЛВС — 100 Мбит/с.

Алгоритмы факторизации тестировались на числах вида $n = pq$, где p, q — простые, так как разложение именно таких чисел на множители является наиболее трудной задачей.

В ходе исследования производилось два вида экспериментов:

- Факторизация чисел n фиксированной разрядности (80 бит) с последовательным увеличением расстояния между множителями p и q от двух до четырёх миллиардов.
- Факторизация чисел n с последовательным увеличением разрядности числа (от 20 до 110 бит), где $p \in \left(0,\ \ n^{1/3}\right]$ — небольшой простой множитель.

В ходе выполнения каждого алгоритма факторизации были последовательно задействованы 1, 2, 4 и 8 процессов, каждый из которых работал на отдельном компьютере, то есть тесты проводились на вычислительной системе с распределённой памятью.

2.1. Метод Ферма

Время нахождения нетривиального делителя (см. рис. 1) числа линейно возрастает с увеличением расстояния между двумя делителями. При этом если делители достаточно близки друг к другу, то разложение происходит относительно быстро. Именно поэтому в асимметричной системе шифрования RSA одним из основных требований является выбор множителей модуля, расстояние между которыми достаточно велико, иначе модуль возможно факторизовать за малое время с помощью метода Ферма, и шифр окажется ненадёжным.

Кроме того, было достигнуто линейное ускорение при увеличении количества процессов, задействованных в нахождении множителя числа.

Для данного метода измерения второго типа с последовательным увеличением разрядности факторизуемого числа не проводились, так как метод Ферма крайне медленно работает с числами, которые содержат малый множитель.

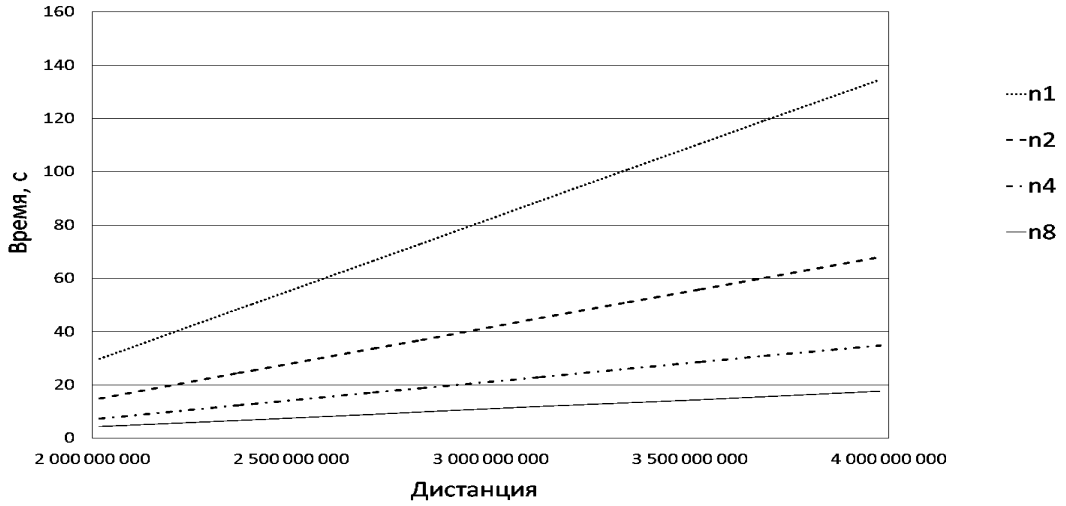

Рис. 1. Результаты измерений для метода Ферма

2.2. Метод Шермана Лемана

Как усовершенствование метода Ферма метод Шермана Лемана также существенно зависит от расстояния между множителями числа (см. рис. 2), время его выполнения линейно зависит от дистанции. Но для таких типов чисел данный алгоритм значительно проигрывает алгоритму Ферма.

Для чисел с небольшим простым делителем ситуация обратная — метод Лемана благодаря последовательным делениям на шаге один достаточно быстро выделит простой множитель (см. рис. 3).

Теоретические результаты совпадают с практическими — получена экспоненциальная зависимость времени выполнения метода Лемана от разрядности факторизуемого числа. Так как простой множитель для чисел разрядности больше 90 бит становится достаточно большим, время его выделения существенно возрастает по сравнению с числами малой разрядности.

Также в ходе исследования было получено линейное ускорение при увеличении количества процессов как для первого вида измерений, так и для второго.

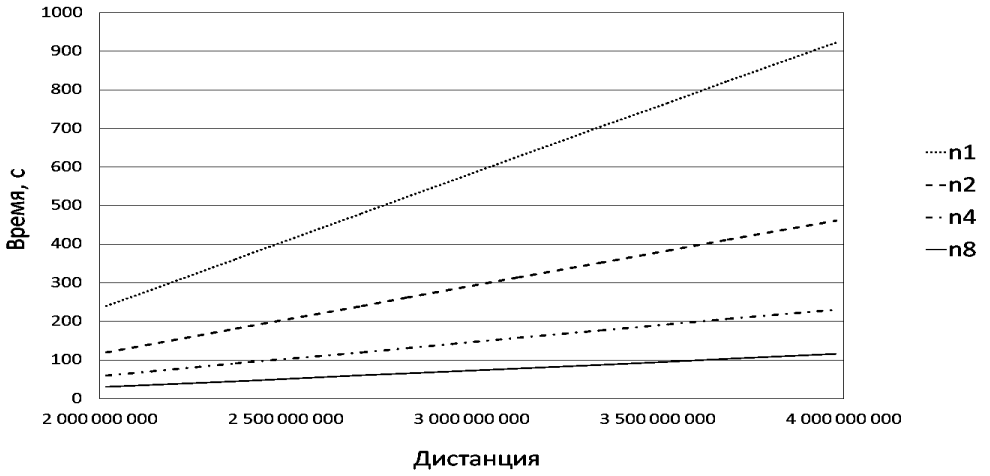

Рис. 2. Результаты измерений для метода Лемана

2.3. Метод Шенкса

Метод Шенкса не зависит от расстояния между сомножителями (см. рис. 4). Время работы данного метода для чисел с фиксированной разрядностью различно.

Для чисел второго типа была получена экспоненциальная зависимость времени работы алгоритма от разрядности (см. рис. 5). С увеличением разрядности сомножителей увеличивается время работы алгоритма, поэтому данный алгоритм подходит лишь для выделения малых простых делителей числа.

2.4. Метод ρ-Полларда

Метод Полларда не зависит от расстояния между сомножителями (см. рис. 6) и для чисел с фиксированной разрядностью выдает примерно одинаковый результат с небольшой погрешностью.

Была получена экспоненциальная зависимость времени работы алгоритма от разрядности числа (см. рис. 6). Для чисел с относительно небольшим множителем метод Полларда показывает наилучшие результаты среди алгоритмов с экспоненциальной сложностью. Линейного ускорения достичь не удалось.

2.5. Метод эллиптических кривых

С увеличением дистанции между множителями величина наименьшего простого множителя уменьшается. Так как время выполнения алгоритма факторизации с эллиптическими кривыми зависит лишь от величины этого множителя, оно постепенно уменьшается с увеличением расстояния между множителями (см. рис. 8). Фактически данные кривые – это небольшие участки экспонент (см. рис. 9).

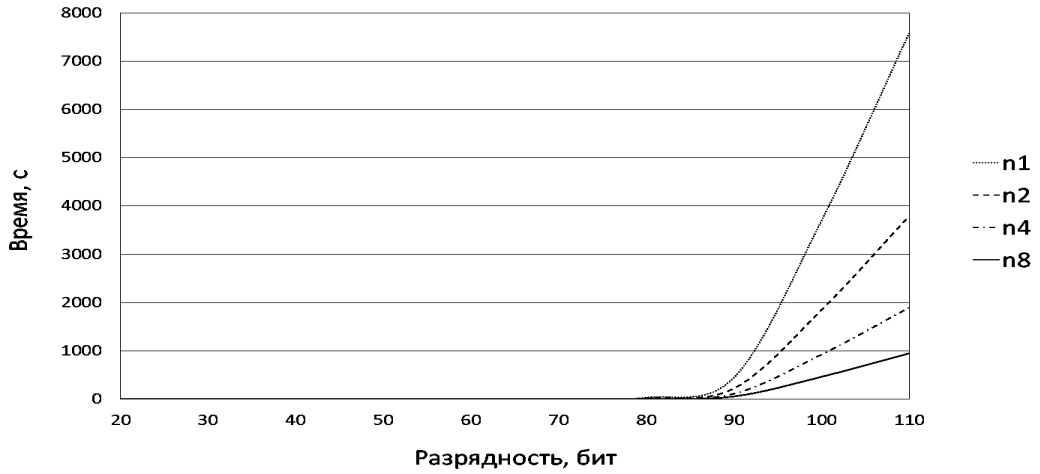

Рис. 3. Результаты измерений для метода Лемана

Ввиду того, что алгоритм вероятностный, и вычисления, связанные с нахождением нетривиального простого делителя числа, возможно, не будут распределены равномерно между процессами, в точности линейного ускорения достичь не удалось, но результаты близки к таковому (см. рис. 9). Также следует отметить, что время выполнения алгоритма значительно меньше по сравнению с любым экспоненциальным алгоритмом, рассмотренным выше.

2.6. Метод квадратичного решета

Для чисел с фиксированной разрядностью время работы алгоритма не меняется в зависимости от разрядности сомножителя (см. рис. 10).

Линейного ускорения достичь не удалось (см. рис. 11), ввиду того что метод квадратичного решета для чисел с разрядностью до 110 бит работал достаточно быстро и на одном процессе, а при распараллеливании алгоритма происходит отправка данных каждым процессом, которая влияет на время работы алгоритма.

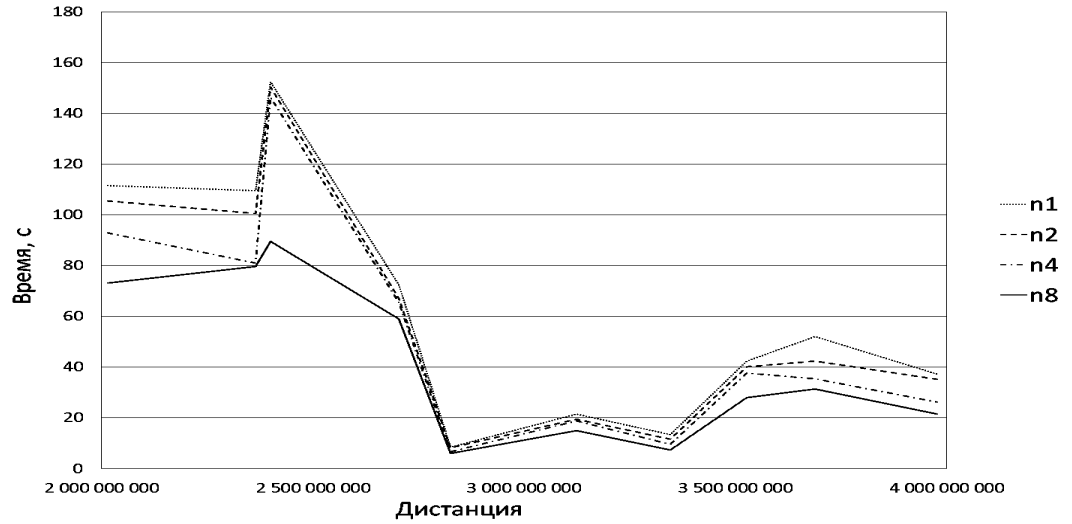

Рис. 4. Результаты измерений для метода Шенкса

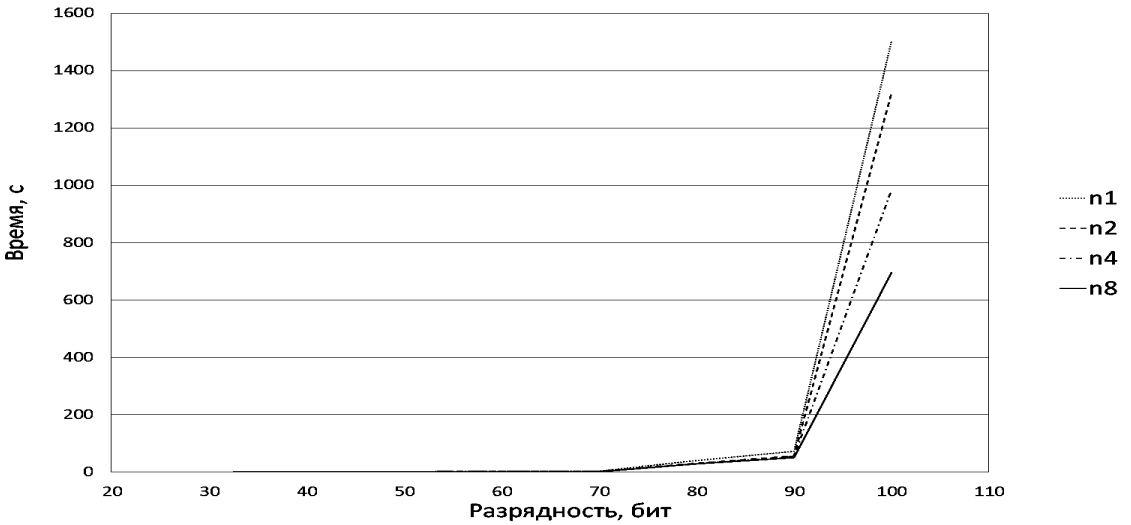

Рис. 5. Результаты измерений для метода Шенкса

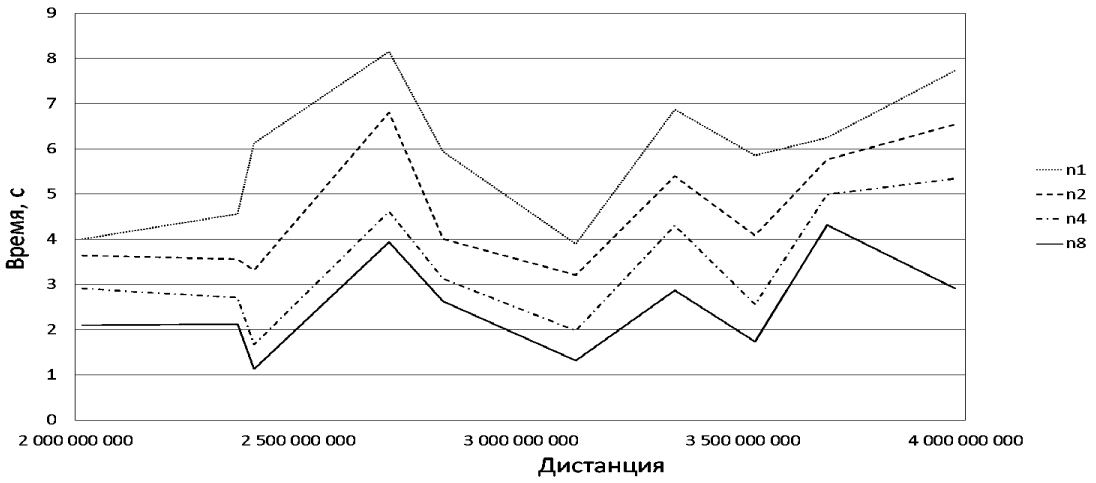

Рис. 6. Результаты измерений для метода Полларда

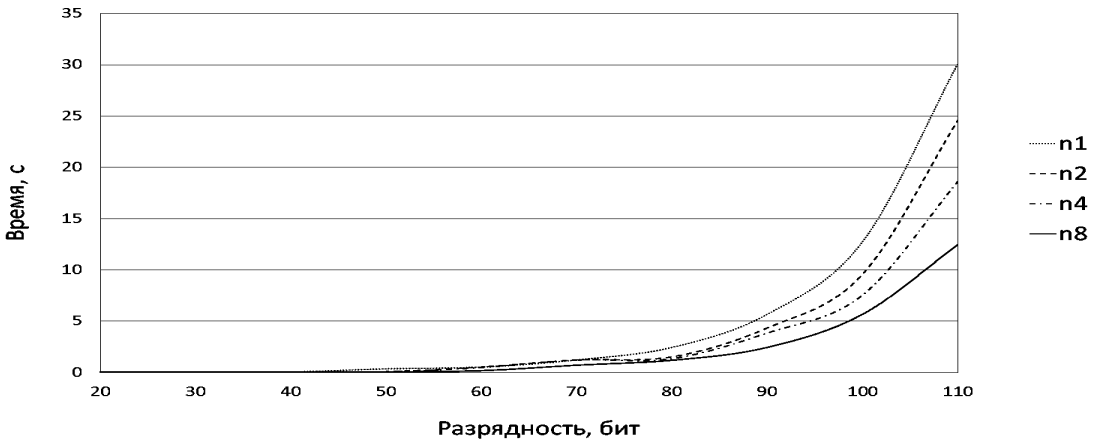

Рис. 7. Результаты измерений для метода Полларда

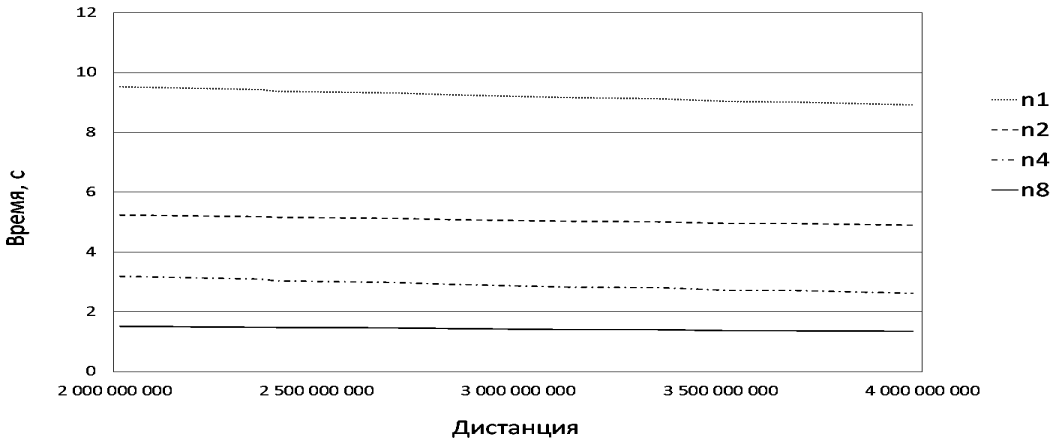

Рис. 8. Результаты измерений для метода эллиптических кривых

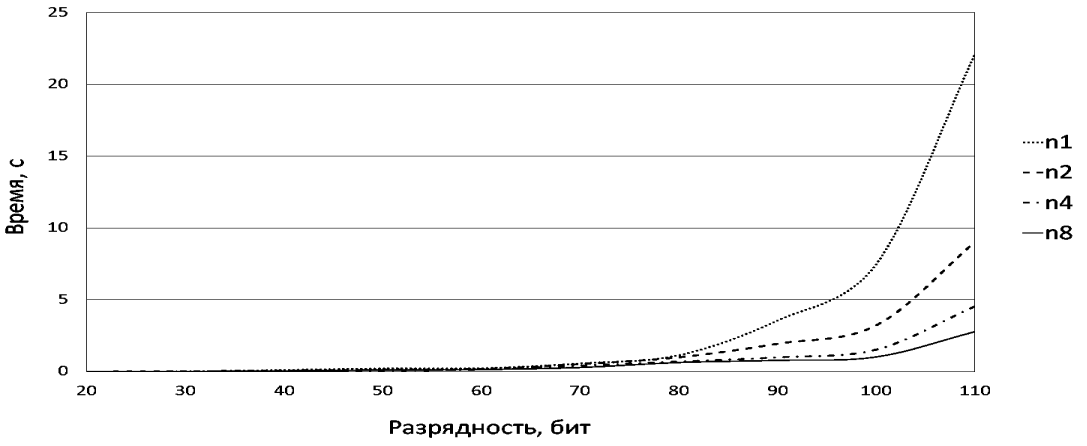

Рис. 9. Результаты измерений для метода эллиптических кривых

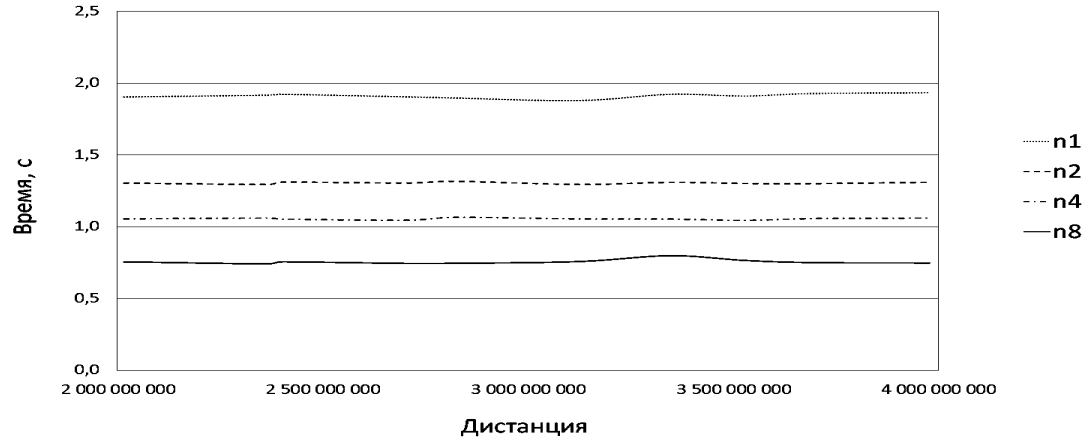

Рис. 10. Результаты измерений для метода квадратичного решета

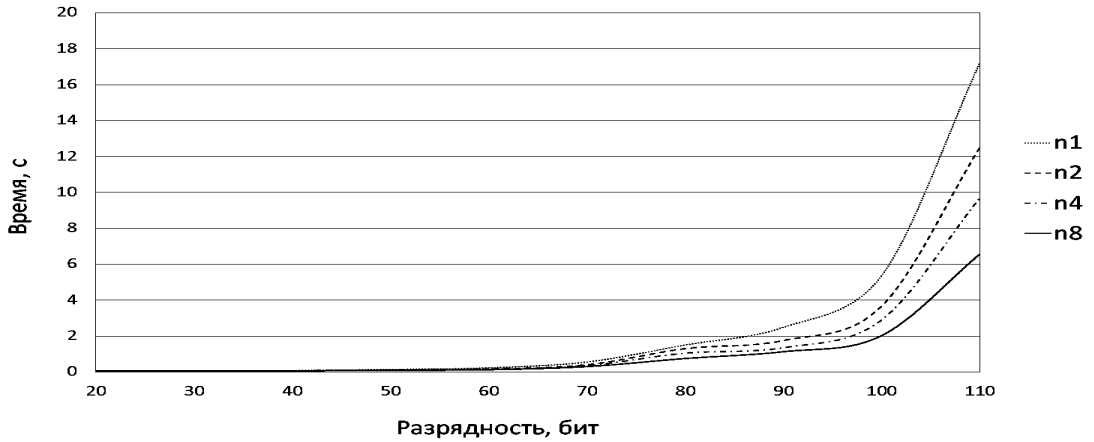

Рис. 11. Результаты измерений для метода квадратичного решета

2.7. Сравнение алгоритмов

Ввиду существенной разницы во времени выполнения экспоненциальных и субэкспоненциальных алгоритмов сравнение произведено в пределах своих категорий.

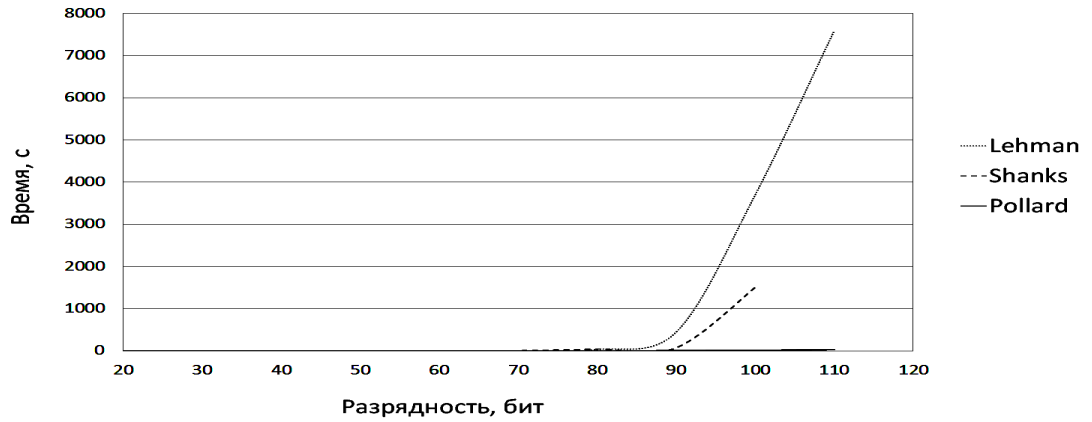

Рис. 12. Сравнение времени выполнения экспоненциальных алгоритмов

Исходя из вычислительной сложности алгоритмов, а также из практических результатов, можно сделать вывод, что в общем случае самым быстрым методом из группы экспоненциальных является метод Полларда (см. рис. 12).

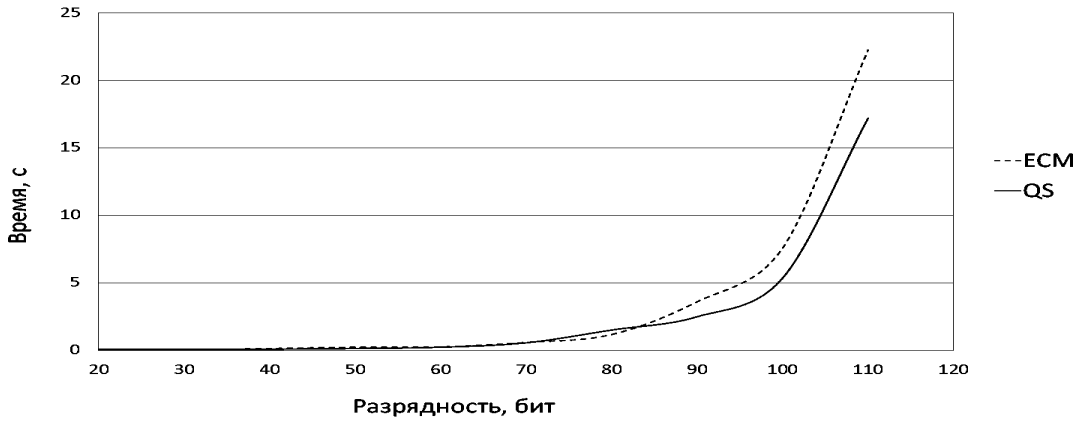

Рис. 13. Сравнение времени выполнения субэкспоненциальных алгоритмов

Очевидно, самым быстрым алгоритмом факторизации среди рассмотренных в исследовании является метод квадратичного решета (см. рис. 13). Погреш-

ность измерений, связанная с небольшим выигрышем метода эллиптических кривых на некоторых числах, исчезнет при увеличении количества измерений.

Заключение

Таким образом, в ходе исследования для большинства алгоритмов было достигнуто линейное ускорение при параллельной реализации. Также при изучении результатов работы алгоритмов было выяснено следующее: при наличии очень близких множителей наиболее эффективен метод Ферма, при относительно небольшом множителе — метод эллиптических кривых, при малых множителях — методы Шенкса и ρ-Полларда; в параллельной реализации наиболее простыми оказались методы эллиптических кривых и ρ-Полларда. В общем случае следует применять метод квадратичного решета.

Дальнейшие исследования могут строиться на основе улучшений существующих последовательных алгоритмов факторизации. Например, для метода эллиптических кривых достаточно эффективным является усовершенствование Монтгомери или использование только проективных координат, благодаря чему в алгоритме не будет использоваться ресурсоёмкое деление по модулю.

Метод квадратичного решета может быть эффективно доработан с помощью так называемой LP-стратегии. Также возможно использование различных полиномов $q(x)$ на разных процессах, участвующих в факторизации. Данные улучшения существенно уменьшат время выполнения алгоритмов.

Литература

1. Brent R.P. Some parallel algorithms for integer factorisation // Lect. Notes in Comp. Sci. 1999. V. 1685. P. 1–22.
2. Kanabar K.A. A Comparison Of Integer Factoring Algorithms. The University of Bath, 2007.
3. Lenstra H.W. Factoring integers with elliptic curves // Ann. Math. 1987. V. 126. P. 649–674
4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М. : МЦНМО, 2003.
5. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие. Казань : Казан. ун-т, 2011. 190 с.
6. Фороузан Б. А. Криптография и безопасность сетей: учебное пособие. М. : Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. 784 с.
7. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М. : МЦНМО, 2002.

Математические структуры и моделирование
2012, вып. 26, с. 110–117

УДК 004.272.2:519.16

ГЕНЕТИЧЕСКИЕ АЛГОРИТМЫ С ЧАСТИЧНОЙ ПАРАЛЛЕЛИЗАЦИЕЙ В СИСТЕМАХ С ОБЩЕЙ ПАМЯТЬЮ НА ПРИМЕРЕ ЗАДАЧИ КОММИВОЯЖЁРА

К.В. Пугин, С.С. Ефимов

Данная статья является описанием опыта частичной параллелизации генетических алгоритмов для решения задачи коммивояжёра. Приведены примеры возможного кода, а также результаты тестов производительности различных вариантов алгоритма. Произведено сравнение вариантов реализации ГА как между собой, так и с эталонными вариантами.

Введение

Один из наиболее трудноразрешимых классов задач — NP-полные задачи. Одной из открытых математических проблем столетия является вопрос — можно ли построить полиномиальный алгоритм для их решения? Но пока ответа нет, и в данный момент для их приближенного решения используются всякие надстройки над полным перебором, одной из которых являются генетические алгоритмы. Генетические алгоритмы построены на основе подражания эволюции: каждый метод решения задачи кодируется набором хромосом (методы кодировки могут быть самыми различными), которые могут скрещиваться, мутировать, а также тестироваться на приспособленность при помощи функции решения задачи, которая называется фитнес-функцией.

Поскольку порядок выполнения операций в генетическом алгоритме строго детерминирован (отбор достойных $\rightarrow$ скрещивание $\rightarrow$ мутация $\rightarrow$ переход к следующему поколению), то не всегда их параллелизация осуществляется тривиально. Существует два подхода к распараллеливанию операций на генетических алгоритмах — полная параллелизация (у каждого потока имеется своя популяция, с которой он работает, и раз в несколько поколений они сообщаются), и частичная параллелизация (операции типа скрещивания, отбора и мутации выполняются параллельно, но слежение за поколениями происходит централизовано в главном потоке).

Цель данной работы — исследовать генетические алгоритмы с частичной параллелизацией на системах с общей памятью на примере условной и безусловной реализаций генетического алгоритма для решения задачи коммивояжёра.

Copyright © 2012 **К.В. Пугин, С.С. Ефимов**
Омский государственный университет им. Ф.М. Достоевского
E-mail: ria.freelander@gmail.com,s_efimov@mail.ru

Задачи — проанализировать доступную информацию по генетическим алгоритмам, возможности их параллелизации и применения, реализовать генетические и специализированные алгоритмы решения задачи коммивояжёра, исследовать их производительность в однопоточном и многопоточном вариантах.

1. Средства и возможности решения

Для работы использованы:

- Технические средства:
  - процессор Intel Core i5-2410m,
  - видеокарта NVIDIA GeForce 520m,
  - 4 GB RAM.
- Фреймворки и языки программирования:
  - C++ (Reference Genetic),
  - OpenMP,
  - CUDA 4.1 (Thrust 1.6),
  - Python (Testing frontends, non-performance parts).

В ходе работы было решено остановиться на частичной параллелизации с условным и безусловным скрещиванием, поскольку данные методы наиболее часто применяются в решении реальных задач при помощи генетических алгоритмов.

Реализовано два примера многопоточного решения задачи коммивояжёра при помощи генетического алгоритма на основе библиотеки Thrust. Один из них решает задачу коммивояжёра при помощи генетического алгоритма на основе маршрутов, выступающих там как хромосомы. Применено условное кольцевое скрещивание (постоянно проверяется условие отсутствия данного города в ребёнке, пункты маршрута выбираются с начального у первого родителя, с конечного — у второго), а в качестве мутации выступает полное перемешивание маршрута. Второй пример: применено классическое скрещивание, при этом каждая перестановка нумеруется в лексикографическом порядке. В качестве мутации выступает генерация случайного номера перестановки. Также эти примеры реализованы и в однопоточном варианте путём замены Thrust на STL.

Пример кода модуля алгоритма (условное скрещивание):

```
__host__ __device__ inline
  animal& animal::interbreed(animal& other)
{
  /* условие для выбора потомка */
  if(partial_calc(matrix,plist,len/2,len)<
     partial_calc(matrix,plist,len,len,len/2))
    for(size_t i=1,c1=len/2; ((i<len-1)&&(c1<len-1)); i++)
    {
      /* проверка на наличие поэлементно */
      if(!(in_place(plist,c1,other.plist[i])))
      {
        plist[c1]=other.plist[i];
        c1++;
      }
    }
  else
  {
    for(size_t i=1,c1=1; ((i<len-1)&&(c1<len/2)); i++)
    {
      /* также поэлементная проверка */
      if (!(in_place(plist,len,other.plist[i],c1)))
      {
        plist[c1]=other.plist[i];
        c1++;
      }
    }
  }
  /*
   *  скрещивание происходит с заменой одного
   *  из родителей для избегания выделения памяти
   *  (на CUDA операция занимает много времени)
   */
  return *this;
}
```

В качестве контрольного реализован алгоритм ближайшего соседа на языке Python, а также тестирующий модуль на том же языке, который подсчитывал время выполнения каждого алгоритма, а также результирующий маршрут и его длину. Каждому из алгоритмов на одной и той же итерации передавался один и тот же граф.

Пример кода (Тестирующий модуль):

```
def main():
  with open("testslv.txt", "w") as f: # Пишется в файл
    writer=("Usual:\tGenetic:\tGenetic(C++):
\tGenetic(OpenMP):\tGenetic(CUDA)\n")
    f.write(writer)
    for i in xrange(23, 10000):
      fgraph = Generate(i); #Генерируется граф
      fgraph_array=Translate(fgraph)
      timed=time.time()
      #Вызывается функция ГА на CUDA с измерением времени
      cuda=GeneticCUDA(fgraph_array, fgraph)
      timecuda=time.time()-timed
      timed=time.time()
      #Вызывается функция ГА на OpenMP с измерением времени
      openmp=GeneticOpenMP(fgraph_array, fgraph)
      timeopenmp=time.time()-timed
      timed=time.time()
      #Вызывается функция ГА на C++ с измерением времени
      geneticc=GeneticC(fgraph_array, fgraph)
      timesingle=time.time()-timed
      timed=time.time()
      #Вызывается функция ближайшего соседа с измерением времени
      usual=SolveUsual(fgraph, 0)
      timeusual=time.time()-timed
      timed=time.time()
      #Вызывается функция ГА на Python с измерением времени
      genetic=SolveGenetic(fgraph, 0)
      timegenetic=time.time()-timed
      with open("testslv.txt", "a+") as f:
        # Все времена пишутся в файл
        writer=("{0}\t{1}\n").format(timeusual, timegenetic,
                                     timesingle,timeopenmp,timecuda)
        f.write(writer)
```

2. Полученные результаты

Пояснения к графику:

1. Наибольшее время выполнения алгоритма на CUDA объясняется простотой фитнес-функции и сетевым законом Амдала.

2. OpenMP позволяет получить в n раз больший выигрыш во времени выполнения (на 4 потоках время сокращается в 4 раза).

Пояснения к графику: Аналогично графику 1, только время выполнения уменьшилось в связи с уменьшением числа ветвлений в алгоритме.

Пояснения к графику:

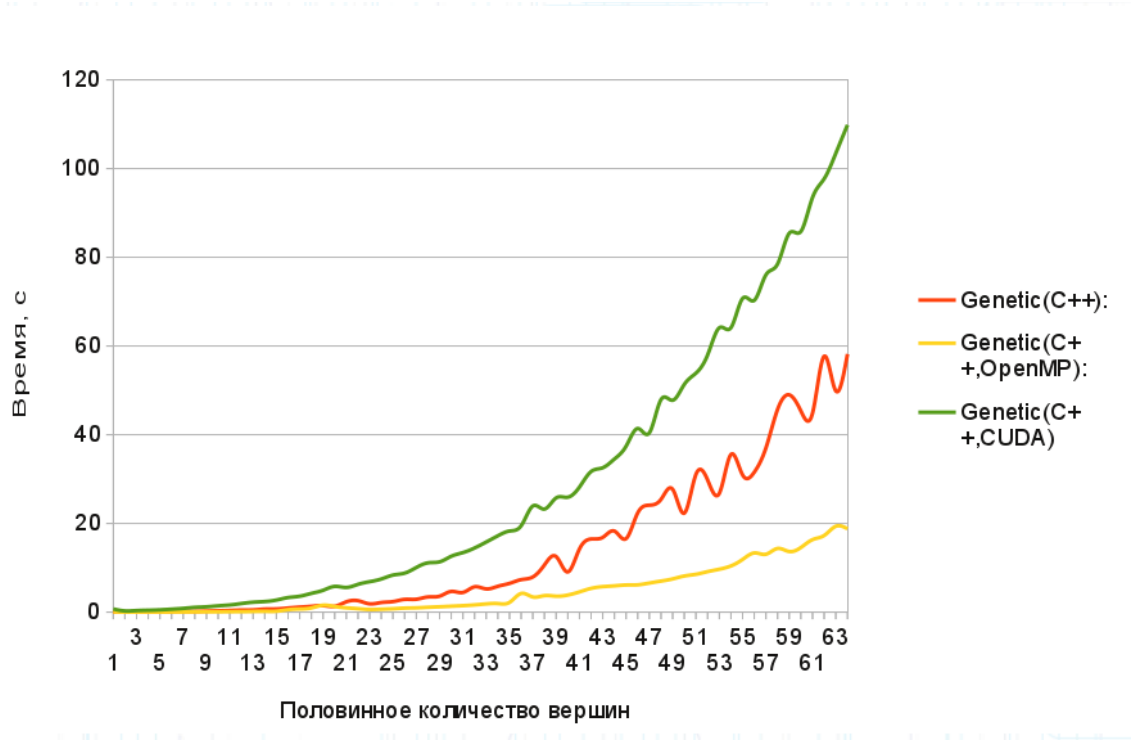

Рис. 1. График производительности условного генетического алгоритма в зависимости от вида параллелизации

1. Алгоритм ближайшего соседа проигрывает в точности генетическому алгоритму при применении на одних и тех же графах.

2. Согласно теореме, для любого количества городов большего трёх в задаче коммивояжёра можно подобрать такое расположение городов (значение расстояний между вершинами графа и указание начальной вершины), что алгоритм ближайшего соседа будет выдавать наихудшее решение [1].

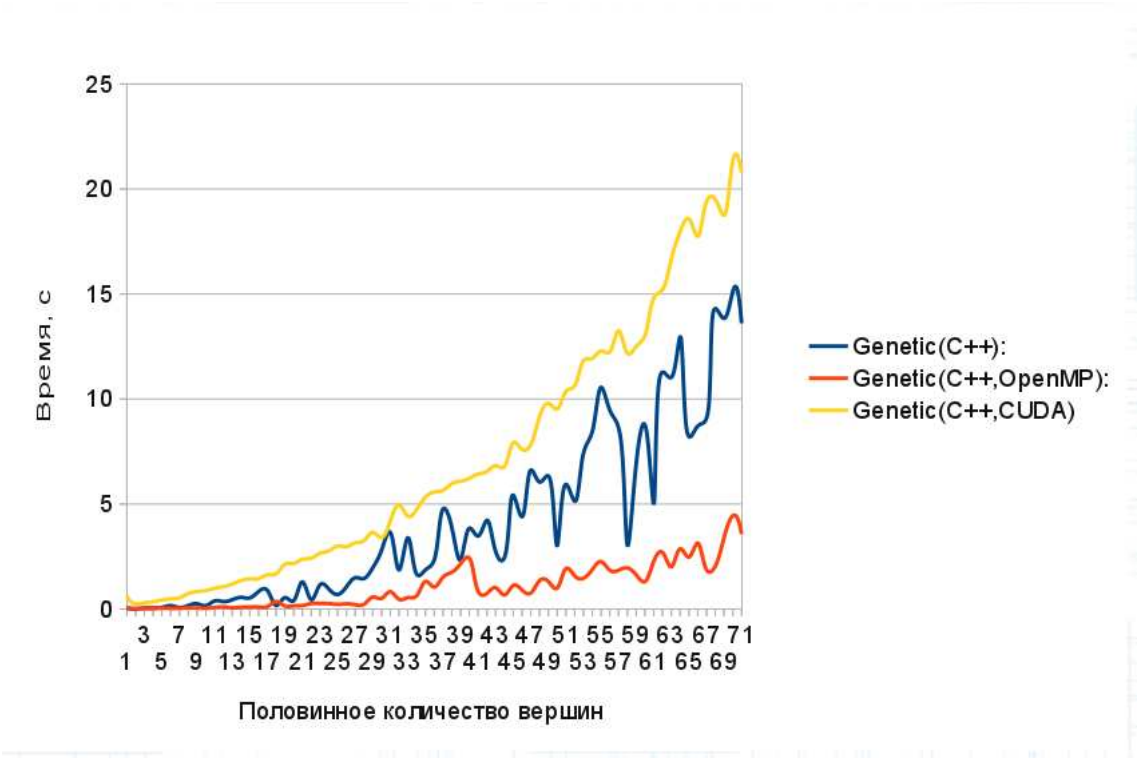

Рис. 2. График производительности безусловного генетического алгоритма в зависимости от вида параллелизации

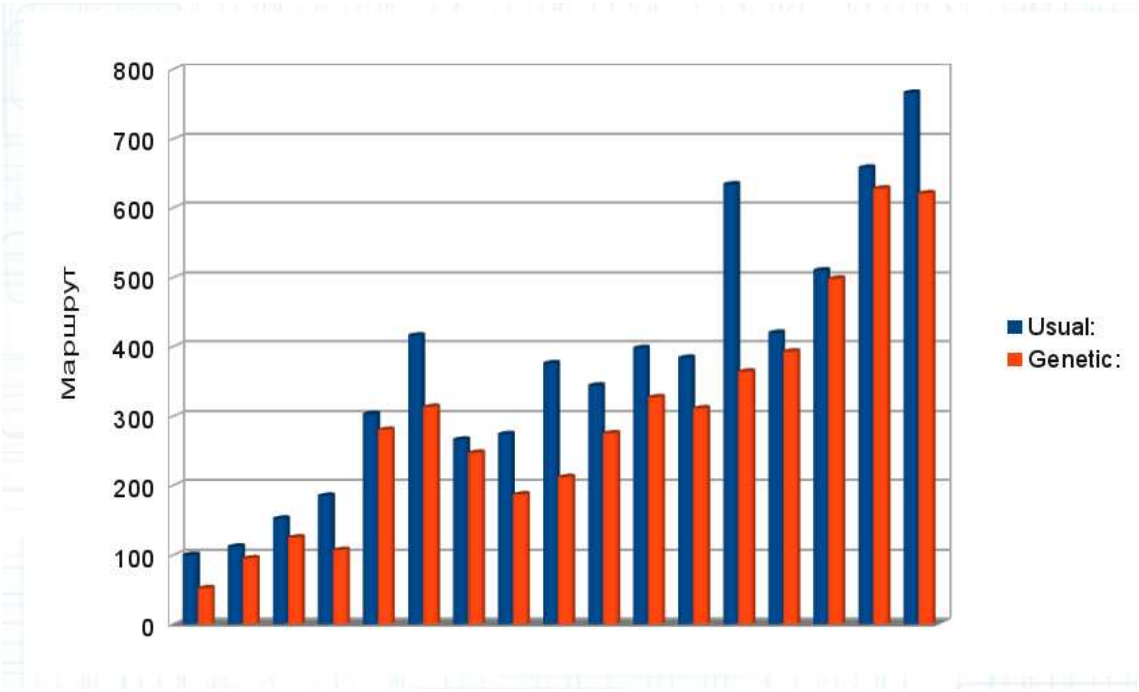

Рис. 3. График точности генетического алгоритма по сравнению с алгоритмом ближайшего соседа

Заключение и общие выводы

Выводы:

1. Применение генетического алгоритма для задачи коммивояжёра полностью оправдано.
2. Для систем параллелизации, использующих пересылки (в частности, для CUDA), критична вычислительная сложность параллельных частей.
3. Частичная параллелизация задачи коммивояжёра позволяет получить выигрыш производительности, сравнимый с количеством ядер.
4. Безусловный алгоритм быстрее для малых графов, но для большого числа вершин их номера не помещаются в восьмибайтную переменную, что влечёт неприменимость решения с нумерацией для большого числа вершин, так как при росте номера преимущества безусловного подхода практически теряются.

Перспективы расширения исследования:

1. Исследование полностью параллельных вариантов генетических алгоритмов с несколькими популяциями.
2. Более полное исследование влияния фитнес-функции и пересылок на производительность ГА.
3. Алгоритмическая оптимизация реализованных алгоритмов (изменение скрещивание под более ускоренный вариант либо под более точный вариант).
4. Программная оптимизация алгоритмов (написание более платформозависимого низкоуровневого кода).

Литература

1. Gutin G., Yeo A., Zverovich A. Traveling salesman should not be greedy: domination analysis of greedy-type heuristics for the TSP. URL: `http://eprints.rhul.ac.uk/archive/00000356/` (дата обращения: 10.09.2012).
2. Debattisti S., Marlat N., Mussi L., Cagnoni S. Implementation of a Simple Genetic Algorithm within the CUDA Architecture. URL: `http://www.gpgpgpu.com/gecco2009/3.pdf` (дата обращения: 10.09.2012).
3. Van Luong Th., Melab N., Talbi E. GPU-based Parallel Hybrid Genetic Algorithms. URL: `http://www.gpgpgpu.com/gecco2010/0.pdf` (дата обращения: 10.09.2012).
4. Shah R., Narayanan P.J., Kothapalli K. URL: GPU-Accelerated Genetic Algorithms. URL: `http://cvit.iiit.ac.in/papers/Rajvi10GPU.pdf` (дата обращения: 10.09.2012).

5. Егоров К., Чураков М. Генетические алгоритмы. URL: http://yury.name/internet/03ia-seminar-note.doc (дата обращения: 10.09.2012).
6. Генетические алгоритмы. От теории к практике. URL: http://habrahabr.ru/post/138091/ (дата обращения: 10.09.2012).
7. Батищев Д.И., Неймарк Е.А., Старостин Н.В. Применение генетических алгоритмов к решению задач дискретной оптимизации. URL: http://www.unn.ru/pages/issues/aids/2007/15.pdf (дата обращения: 10.09.2012).

Математические структуры и моделирование
2012, вып. 26, с. 118–123

УДК 004.93'12

РАСПОЗНАВАНИЕ ДОРОЖНОЙ РАЗМЕТКИ НА БАЗЕ INTEL OPENCV

С.В. Стопкин, К.В. Пугин, С.С. Ефимов

В данной статье производится анализ методов распознавания дорожной разметки, а также приводится простой пример реализованного метода, перспективы развития распознавания разметки при помощи интеграции других методов.

Введение

Ни для кого не секрет, что разработка систем ориентации на дороге и распознавания дорожной разметки идёт в мире с большой скоростью. Крупные IT-компании в сотрудничестве с производителями автомобилей разрабатывают такие системы для обеспечения большей безопасности движения, что в конечном итоге приведёт нас к полностью автоматизированным системам, не требующим какого-либо вмешательства водителя и исключающим пресловутый человеческий фактор. Команда разработчиков состоит из нескольких студентов третьего курса факультета компьютерных наук Омского государственного университета им. Ф.М. Достоевского. Ранее эта же команда представляла и реализовывала смежные проекты по разработке системы наблюдения и контроля за автономными устройствами. Целью проекта является разработка совместимой, кроссплатформенной программно-аппаратной платформы автономного управления транспортом.

Для этого должны быть решены следующие задачи:

1. Разработка необходимых библиотек для компьютерных программ в системах автономного управления транспортом.
2. Разработка необходимых библиотек для компьютерных программ в системах распознавания дорожной разметки.

Также необходимо исследование с целью поиска аналогичных систем обработки изображений, различных методик распознавания. Кроме того требуется проведение большого объёма практических испытаний.

Наработки данного проекта могут быть интересны производителям автомобильного навигационного оборудования и различных систем автомобильной электроники.

Copyright © 2012 **С.В. Стопкин, К.В. Пугин, С.С. Ефимов**
Омский государственный университет им. Ф.М. Достоевского
E-mail: stopkin.sergey@gmail.com, ria.freelander@gmail.com, s_efimov@mail.ru

При разработке использовались материалы следующих источников [1–4]. Уникальность проекта:

1. Создание именно открытой для других разработчиков системы автономного управления транспортом позволит привлечь большее количество участников для внесения улучшений, тестирования и отладки.

2. Использование в проекте технологий параллельных вычислений (OpenCV (vs CUDA/OpenMPI)).

3. Использование технологий Intel: инструменты, библиотеки, платформы, а именно Intel OpenCV и платформа Intel.

4. Масштабируемость: возможно добавление фильтров на другие объекты. Возможно распознавание произвольных типов объектов.

5. Переносимость: результаты проекта применимы на всех аппаратно-программных платформах, на которых возможна сборка кроссплатформенного фреймворка Qt и кроссплатформенной библиотеки «компьютерного зрения» OpenCV.

1. Возможные методы реализации распознавания линий.

1. Метод гистограмм:
   (a) Превращение изображения в черно-белое.
   (b) Применение предельного преобразования в двухцветную картинку. Значение границы вычисляется по алгоритму OTSU.
   (c) Поиск гистограммы.
   (d) Поиск паттерна БЧБ на предсказанных линиях.
   (e) Делается вывод о линии из положения паттерна.

2. IPT (Inverse Perspective Transform):
   (a) Получение преобразования перспективы через размер камеры.
   (b) Превращение изображения в черно-белое.
   (c) Преобразование перспективы для получения вида сверху.
   (d) Применение предельного преобразования в двухцветную картинку. Значение границы вычисляется по алгоритму OTSU.
   (e) Применение алгоритма Канни для распознавания границ.
   (f) Применение линейного преобразования Хаффа для поиска прямых линий (вертикальных).
   (g) Разворот полученных линий в исходную перспективу.

3. RANSAC и логарифмическое полярное преобразование координат:

(a) Превращение изображения в черно-белое.

(b) Применение предельного преобразования в двухцветную картинку. Значение границы вычисляется по алгоритму OTSU.

(c) Применение алгоритма Канни для распознавания границ.

(d) Логарифмическое полярное преобразование координат.

(e) Применение параболического поиска RANSAC.

(f) Обратное преобразование линий на картинку.

4. Алгоритм B-Shake:

(a) Превращение изображения в черно-белое.

(b) Применение предельного преобразования в двухцветную картинку. Значение границы вычисляется по алгоритму OTSU.

(c) Применение алгоритма Канни для распознавания границ.

(d) Построение сенсоров (количество выбирается опытным путём).

(e) Каждый сенсор выполняет линейное преобразование Хаффа для поиска двух сходящихся прямых линий, возвращая точку схождения.

(f) По найденным точкам и по центральной точке внизу изображения строят модель средней линии.

(g) По модели средней линии и найденным на каждом сенсоре линиям строим модель полосы.

5. Преобразование Хаффа с поиском сходящихся линий:

(a) Превращение изображения в черно-белое.

(b) Применение предельного преобразования в двухцветную картинку. Значение границы вычисляется по алгоритму OTSU.

(c) Применение алгоритма Собеля для распознавания границ.

(d) Применение линейного преобразования Хаффа для поиска прямых линий.

(e) Эвристика для поиска двух сходящихся параллельных линий, а также сохранения их положения при потере одной из них.

6. Совмещение методов B-Shake sensors и Sobel (метод в разработке).

2. Реализация — разработка и перспективы

1. Стадия ранней разработки системы. Исследование методов, которые возможно применить для решения поставленной задачи и реализации системы в целом. Выбраны следующие методы для проекта:

(a) Преобразование Хаффа с поиском сходящихся линий (реализовано) — даёт хороший результат на прямых изображениях,

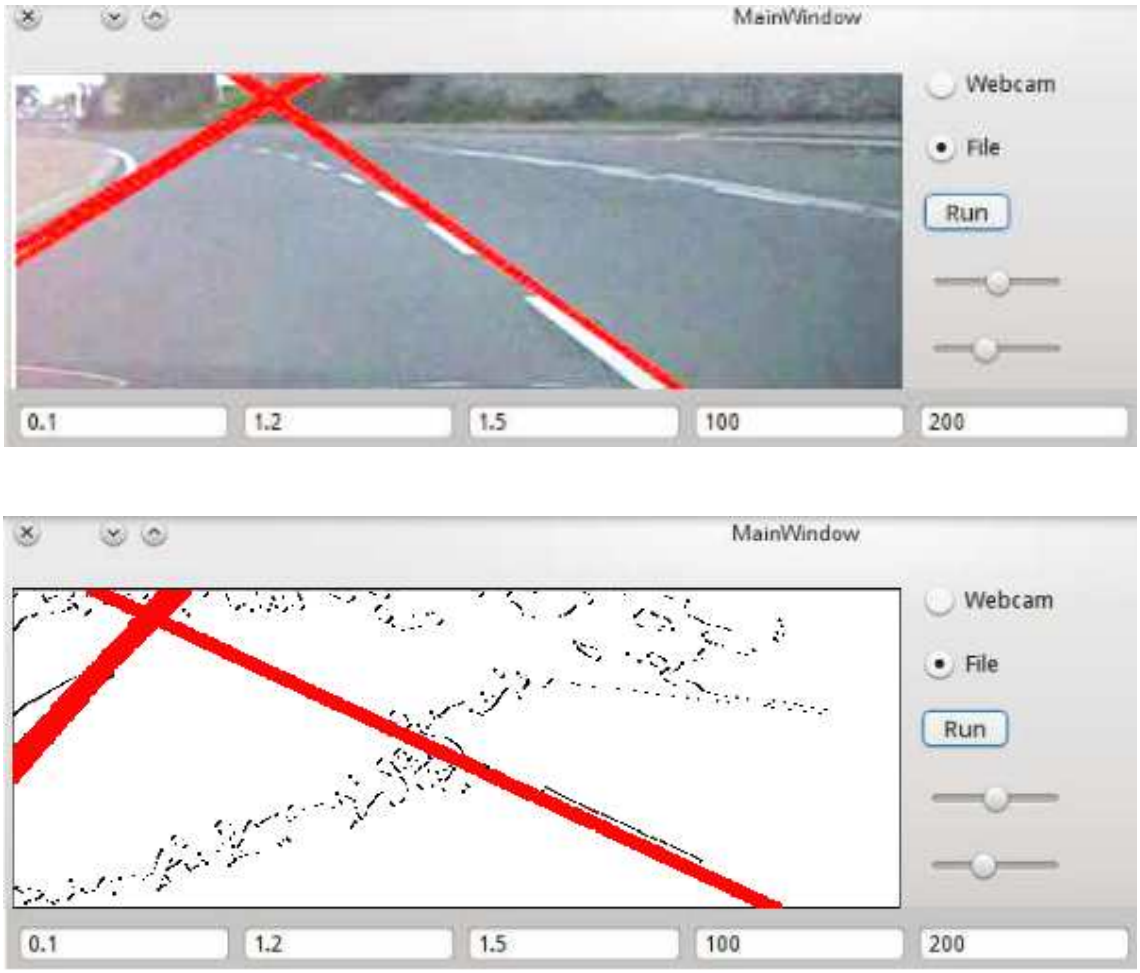

Рис. 1. Скриншоты работы программы — видео в исходном и преобразованном видах

(b) B-Shake — это расширение предыдущего метода, даёт очень хорошие результаты, при этом есть планы по его доработке.

2. Пример реализации простого метода:

```
vector <cv::Vec2f> LaneSensor::processImageS(cv::Mat hsv){
    hsv=hsv(Region);
    cv::Mat bgr;
    // BGRing image
    cv::cvtColor (hsv,bgr,CV_HSV2BGR);
    cv::Mat gray_image;
    cv::Mat old_gray;
    // Grayscaling image
    cv::cvtColor (bgr,old_gray,CV_BGR2GRAY);
    vector <cv::Mat> h_s_v;
    cv::split(hsv,h_s_v);
    gray_image=old_gray.clone();
    // Apply Blur to get rid from noise
```

```
    cv::GaussianBlur(gray_image,gray_image,cv::Size(3,3),0,0);
    // OTSU Thresholding
    cv::threshold(gray_image,gray_image,t1,t2,cv::THRESH_OTSU);
    // Sobel edge detector
    cv::Sobel(gray_image,gray_image,0,1,1);
    // Dilation
    cv::dilate(gray_image,gray_image,cv::Mat());
    // Hough transform
    cv::HoughLines(gray_image,lines,1,CV_PI/180,h1);
    // Angle to approval
    lines=TestLinesAngleS(lines,CV_PI/4,CV_PI/2.25);
    // Returning sensor result
    return lines;
}
```

3. Стадия разработки тестовых приложений для отладки алгоритмов проекта. Скриншоты, демонстрирующие работу тестового приложения — обработка видеозаписи, на которой присутствует дорога с разметкой по методу преобразования Хаффа, представлены на рисунке 1.

4. Разработка алгоритма B-Shake — реализованы часть сенсоров, частичное распознавание линий. В разработке — построение профиля дороги по данным каждого сенсора.

3. Заключение. Достигнутый и ожидаемый результат

Достигнутый результат — реализован один из базовых методов распознавания разметки на дороге. Ожидаемый результат — реализация комплексного метода распознавания разметки (на основе B-Shake, IPT и поиска сходящихся линий). Коммерческая привлекательность проекта: использование наработанного кода и данных в бортовых ПК автомобилей и иного транспорта. При наличии совместимой аппаратной платформы и необходимых библиотек возможно использование в любых системах, где это необходимо. Наиболее перспективно развитие методов распознавания линий там, где недостаточно данных о положении камеры и дороги. В данном случае и применяются рассмотренные методы.

Литература

1. Wang Y., Teoh E.K., Shen D. Lane detection and tracking using B-Snake. URL: http://www1.i2r.a-star.edu.sg/~ywang/papers/IVC_lane%20detection%20and%20tracking%20using%20bsnake.pdf (дата обращения: 15.09.2012).
2. Kim J., Jang J. A simple model for a lane detection system. URL: http://spie.org/x85441.xml (дата обращения: 15.09.2012).

3. Контурный анализ. URL: http://habrahabr.ru/post/118486/ (дата обращения: 15.09.2012).
4. Bradski G., Kaehler A. Learning OpenCV. URL: http://www.cse.iitk.ac.in/users/vision/dipakmj/papers/OReilly%20Learning%20OpenCV.pdf(дата обращения: 15.09.2012).

Математические структуры и моделирование
2012, вып. 26, с. 124–134

УДК 612.087.1:004.056.523

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ЛИЧНОСТИ: ОБЗОР ОСНОВНЫХ БИОМЕТРИЧЕСКИХ МЕТОДОВ ПРОВЕРКИ ПОДЛИННОСТИ ПОЛЬЗОВАТЕЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ

А.Б. Лысак

В статье рассматриваются основные биометрические методы, применяемые в современных компьютерных системах в целях идентификации и аутентификации пользователя. Приводится базовая классификация методов и описываются сферы их применения и ключевые отличия.

Введение

Необходимость разграничения доступа к постоянно возрастающим объёмам информации в современном мире остро ставит проблему проверки подлинности пользователя. Рост компьютерных сетей и интенсивности их использования также упрощает задачу злоумышленника по получению несанкционированного доступа к данным или определённым сервисам, предоставляемым компьютерными системами.

Помимо обеспечения разграничения прав доступа к конфиденциальной информации современные автоматизированные комплексы решают ряд смежных задач. Двумя основными процедурами, выполняемыми подобными комплексами, являются идентификация и аутентификация субъекта доступа. В общем случае таким субъектом для компьютерной системы может являться не только человек, но и любой процесс, выполняемый удалено или локально [1].

Однако по данным анализа статистики экспертами в области компьютерной безопасности большинство случаев, связанных с утечками информации связаны с факторами, к которым напрямую причастен человек. Причинами доступа третьих лиц к конфиденциальной информации на порядок чаще становилась работа инсайдеров и хакеров, нежели действия зловредного программного обеспечения [2, 3]. Таким образом, выводы экспертов подтверждают первостепенную значимость проблемы идентификации и аутентификации личности в области компьютерной безопасности.

В большинстве современных компьютерных систем проверка личности пользователя осуществляется с помощью ввода логина и пароля. В настоящее время

Copyright © 2012 **А.Б. Лысак**
Омский НИИ приборостроения
E-mail: antonlysak@gmail.com

существуют и другие методы, которые, хотя и не получили такого широкого распространения, потенциально являются намного более надёжными. В частности, существует целый класс перспективных биометрических подходов.

Целью данной статьи является нахождение способа надёжной защиты от несанкционированного доступа к информации путём применения современных биометрических технологий.

Для достижения данной цели необходимо:

1. Проанализировать существующие подходы к идентификации и аутентификации личности.

2. Рассмотреть современные биометрические технологии, их сильные и слабые стороны.

3. Найти приемлемую технологию или их комбинацию, которые бы обеспечили более надёжную защиту конфиденциальной информации.

1. Современные подходы к идентификации и аутентификации

В первую очередь необходимо определить различия между идентификацией и аутентификацией.

Процесс идентификации заключается в предъявлении пользователем идентификатора и сопоставления его с образцами идентификаторов всех пользователей в системе (сравнение 1:m). Наибольшее распространение чистая идентификация получила областях, где непосредственный контакт человека с системой не предусмотрен, например, в системах распознавания лиц. В качестве проверки личности пользователя при доступе к ресурсам современных компьютерных систем идентификация не используется по причинам значительно меньшей надёжности по сравнению с аутентификацией.

В процессе аутентификации пользователь также должен предъявить системе идентификатор, заявляя о том, кто он, и подтвердить свою личность. Для этого в дополнение к идентификатору используется нечто, называемое не получившим широкого распространения термином *аутентификатор*. После нахождения в базе данных требуемой записи о пользователе с помощью идентификатора, система выполняет сравнение аутентифакотора, хранящегося в ней с тем, который предъявил пользователь. При аутентификации последовательно выполняется сравнение 1:m идентификаторов и 1:1 аутентификаторов.

Таким образом, для того, чтобы система функционировала с требуемыми уровнями быстродействия и надёжности, необходимо правильно выбирать, что использовать в качестве идентификатора, а что — в качестве аутентификатора.

Три основных подхода, с помощью которых возможно осуществить как идентификацию, так и аутентификацию, описаны ещё в 1994 году [4]:

1. С использованием собственности — пользователь предъявляет системе некоторый физический предмет, например, смарт-карту или usb-токен.

2. С использованием знаний — пользователь вводит в систему какую либо секретную фразу, например, пароль или PIN-код.

3. С использованием характеристик — пользователь предъявляет системе свои физиологические или поведенческие параметры.

Автор статьи, Бенджамин Миллер, рассматривая эти три подхода, говорил об их совместном использовании. Например, при доступе к своему банковскому счету с помощью банкомата пользователь использует пластиковую карту (собственность) в качестве идентификатора и PIN-код (знания) в качестве аутентификатора. В настоящее время первые два подхода широко применяются как в комбинации, так и по отдельности. Помимо специализированных систем аутентификация с использованием собственности в виде USB-брелока возможна на персональном компьютере с операционной системой общего пользования [5]. Тем не менее, наиболее широкое распространение получил подход с использованием знаний в чистом виде. Связка: логин в качестве идентификатора и пароль в качестве аутентификатора — ежедневно используется сотнями миллионов пользователей глобальной сети Интернет по всему миру. В качестве основной причины повсеместного распространения данного подхода можно, в первую очередь, выделить отсутствие необходимости в дополнительном аппаратном обеспечении для проведения процедуры аутентификации и, как следствия этого, отсутствие дополнительных материальных затрат и более высокий уровень удобства пользователя.

Несмотря не невысокую распространённость биометрических характеристик, неоспоримыми преимуществами их использования является то, что их, в отличие от собственности и знаний, невозможно намеренно передать другому, потерять или украсть. Данные свойства биометрических характеристик делают их практически идеальными для использования в качестве аутентификатора, поскольку надёжность системы аутентификации напрямую зависит от возможности его попадания в руки злоумышленника.

В это же время использование биометрических характеристик в качестве идентификатора сопряжено с некоторыми трудностями. Проблема заключается в том, что в отличие от знаний и собственности предъявляемый пользователем биометрический идентификатор никогда не будет с абсолютной точностью совпадать с идентификатором из базы данных. В процессе экстракции свойств из биометрического образца они подвергаются искажению и наложению шума [6]. Это приводит к тому, что при поиске соответствующего биометрического идентификатора в базе данных используется не простое сравнение цифрового представления информации, а более сложный алгоритм:

1. К образцу, предъявляемому пользователем B_1, и хранящемуся в базе данных B_2 применяется функция экстракции — $f(B_1)$, $f(B_2)$.

2. Вычисляется величина, выражающая степень сходства между образцами $s(f(B_1), f(B_2))$.

3. Получившаяся величина сравнивается с заранее заданным пороговым значением T. В случае $s > T$ процедура завершается успешно, в случае $s < T$ — неудачно.

Эффективность работы алгоритма применительно к выбранному биометрическому параметру обычно оценивают по двум критериям:

1. FAR(False Acceptence Rate) — коэффициент ложного доступа, процентный показатель случаев, при которых проверка личности оказалась ошибочно успешной.

2. FRR(False Rejection Rate) — коэффициент ложного отказа в доступе, процентный показатель случаев, при которых проверка личности ошибочно завершилась неудачей.

Для использования биометрического идентификатора в системе аутентификации необходимо применение биометрического параметра B, функций экстракции f и сравнения s, для которых требования к вычислительным ресурсам будут минимальными при достаточно низком уровне FRR. Это должно обеспечить быстрое и успешное определение личности пользователя. При этом требование по минимизации FAR не является критичным, поскольку надёжность аутентификации практически полностью зависит от аутентификатора, а не от идентификатора. Для повышения удобства процедуры аутентификации также возможно использование нескольких различных типов идентификаторов для каждого пользователя. Внедрение гибридных систем аутентификации, в которых пользователь может использовать биометрические параметры по своему выбору вместо традиционного ввода логина не влияет на безопасность и при этом позволяет совершить плавный переход к широкому использованию биометрии.

Если для идентификатора наиболее важным параметром является FRR, то при выборе подходящего аутентификатора критичную роль играет значение FAR. Помимо этого, рост применения биометрических аутентификаторов также возможен только при выполнении определённых требований, которые будут рассмотрены далее.

2. Основные биометрические методы и их классификация

Все биометрические параметры можно разделить на две большие группы:

1. Физиологические — физические характеристики человека, измеряемые в определённый момент времени;

2. Поведенческие — определённые действия, совершаемые человеком на протяжении промежутка времени.

В настоящее время подавляющее большинство систем аутентификации использует в качестве биометрических параметров физиологические признаки.

Причиной этого можно назвать значительно более высокую надёжность по сравнению с поведенческими характеристиками при достаточно несложных алгоритмах экстракции и вычисления сходства. В то же время, наибольшее распространение получили не самые эффективные подходы по показателям FAR/FRR. Проанализировав ситуацию, можно выделить следующие основные факторы, влияющие на применимость того или иного биометрического метода:

1. Стоимость оборудования для получения требуемой биометрической характеристики.

2. Возможность подделки биометрического образца злоумышленником.

3. Удобство, которое складывается из среднего времени, занимаемого процедурой, и перечнем действий, совершаемых в её процессе.

4. Отношение общества к использованию данной характеристики.

Поскольку при достаточно большом разнообразии подходов дать количественную оценку по каждому из данных факторов не представляется возможным, необходимо попытаться качественно оценить основные биометрические методы, используемые в настоящее время и имеющие потенциальную применимость в ближайшем будущем. В статье принципиально не рассматриваются такие методы как использование ДНК или сетчатки глаза, поскольку оборудование для их получения настолько дорогостоящие, что не приходится предполагать рост распространения данных подходов.

Отпечатки пальцев

Использование отпечатков пальцев берет своё начало в конце XIX века и основывается на гипотезе Уильяма Гершеля о том, что папиллярные линии на поверхности ладоней и пальцев являются уникальными для каждого человека. Несмотря на то, что это предположение до сих пор не имеет научного обоснования, с начала XX века и по настоящее время данный биометрический признак получил широкое распространение в целях идентификации преступников. Кроме того, сейчас он также является наиболее часто используемым биометрическим признаком для предоставления доступа к компьютерным системам. Более 12% моделей современных ноутбуков имеют встроенные аппаратные и программные средства для получения и обработки отпечатков пальцев.

В настоящее время для получения отпечатка пальца используются специальные сканеры. Все существующие сканеры можно разделить на три группы [7]:

1. Оптические.

2. Полупроводниковые.

3. Ультразвуковые.

Оптические сканеры основаны на использовании оптических методов получения изображения. Существует несколько способов реализации данного метода, но общий принцип заключается в том, что небольшая камера или набор фотодатчиков фиксируют изображение на специальной полупрозрачной поверхности, получаемое в результате освещения пальца с одной или нескольких сторон. Стоимость таких сканеров на рынке начинается с 15$. Процедура получения отпечатка занимает не более секунды и производится в одно касание. К минусам данных устройств можно отнести отсутствие защиты от муляжей и быстрое загрязнение сканера, резко понижающее его надёжность.

В основе работы полупроводниковых сканеров лежит использование особых свойств полупроводников, изменяющихся в местах контакта гребней папиллярного узора с поверхностью сканера. Можно выделить следующие типы данных устройств:

1. Ёмкостные.
2. Радиочастотные.
3. Пьезоэлектрические.
4. Термические.

Ёмкостные и пьезоэлектрические сканеры имеют сопоставимые с оптическими сканерами стоимость и надёжность. Радиочастотные и термические являются гораздо более устойчивыми к атакам с использованием муляжей, но имеют более высокую стоимость.

Ультразвуковые сканеры являются относительно новыми на рынке устройств получения отпечатков пальцев. Они используют ультразвуковые волны для облучения поверхности пальцев и определяют папиллярный узор по отражённому эху. Качество получаемых изображений в несколько раз выше, чем у оптических и полупроводниковых сканеров. Данный способ практически полностью защищён от муляжей и устойчив к загрязнению пальцев. Существенным недостатком является высокая стоимость подобных устройств по сравнению с оптическими и полупроводниковыми сканерами.

Вне зависимости от применяемых устройств отпечаток пальца, как и практически любой другой физиологический признак, может без особого труда быть получен злоумышленником. Изготовить муляж также не представляет особой технической сложности, в особенности для обмана широкораспространенных недорогих моделей сканеров. Второй проблемой является то, что в случае компрометации сменить изображение отпечатка пальца в отличие от пароля не представляется возможным. Кроме того реакция современного общества на повсеместное использование отпечатков пальцев определённо является негативной по причине применения данного признака в криминалистике.

Лицо

Методы проверки подлинности с использованием изображения лица стали стандартом де-факто ещё до широкого распространения компьютерных систем.

Так практически все документы, удостоверяющие личность, содержат фотографию лица аутентифицируемого субъекта. Этот способ распознавания является наиболее естественным для человека и поэтому не встречает никакого сопротивления со стороны общества.

Достаточно надёжные системы базируются на применении нескольких камер, расположенных под разными углами и обеспечивающих формирование трёхмерной модели лица. В них также используется дополнительная подсветка для снижения влияния освещения на получаемый результат. Подобные системы находят применение на контрольно-пропускных пунктах предприятий. В то же время применение таких систем обычными пользователями в повседневных условиях невозможно по причине их высокой стоимости, сложности установки и использования.

Наиболее распространёнными устройствами, позволяющими получить двухмерное изображение лица пользователя являются веб-камеры. В настоящее время около 95% моделей ноутбуков, представленных на рынке, имеют встроенную камеру. Стоимость внешней веб-камеры для персонального компьютера составляет от 10$. Использование недорогого оборудования негативно сказывается на надёжности системы. Отрицательное влияние также оказывает изменяющееся освещение.

Современные алгоритмы способны компенсировать наличие очков, усов и бороды, а также дополнительных аксессуаров на лице исследуемого индивида даже на двумерном изображении. Однако основной проблемой использования двумерных изображений является уязвимость к атакам с использованием муляжей. Для обмана таких систем достаточно использование фотографии субъекта.

Соответственно, можно сделать вывод о том, что широкое распространение может получить только подход с использованием двумерного изображения лица в качестве идентификатора.

Ладонь

С руки человека возможно собрать до 90 информационных признаков [8]. Однако не все они в настоящее время используются.

Существует два подхода при использовании изображения ладони:

1. Первый, существующий с 1976 года, основан исключительно на геометрических характеристиках кисти.

2. Второй, современный, использует кроме геометрических ещё и рисунки на сгибах между фалангами пальцев и узоры кровеносных сосудов.

Современные сканирующие устройства не требуют непосредственного контакта ладони с поверхностью сканера. Соответственно, при их использовании не предъявляется жёстких требований к чистоте, влажности, температуре рук. Процедура сканирования занимает несколько секунд, удобна для пользователя, а сам метод не встречает негативной реакции со стороны общества.

Получение данных злоумышленником и изготовление муляжа, особенно для систем, использующих исключительно геометрические характеристики, не является неразрешимой задачей, хотя и более сложно, чем в случае с отпечатками пальцев или изображением лица. Существенным недостатком также является высокая стоимость устройств сканирования — около 300$, не включая затрат на программное обеспечение [9]. В настоящее время это является важнейшим сдерживающим фактором для распространения данного биометрического метода.

Радужная оболочка глаза

Радужная оболочка глаза является уникальной характеристикой человека. Её рисунок формируется на восьмом месяце внутриутробного развития, окончательно стабилизируется в возрасте около двух лет и практически не изменяется в течение жизни, кроме как в результате сильных травм или резких патологий. Данный метод в настоящее время является одним из наиболее точных [10].

Качество современных устройств получения изображения радужной оболочки в совокупности с разработанными алгоритмами позволяет достигать достаточной надёжности для использования данного метода в режиме чистой идентификации. [11] Однако стоимость устройств, позволяющих получить настолько качественные изображения, составляет несколько тысяч долларов США и ограничивает их применение организациями, в которых предъявляются очень высокие требования к безопасности. Также существуют реализации систем на базе простых и дешёвых цифровых фотокамер с высоким разрешением, однако их надёжность является более низкой.

С точки зрения удобства для пользователя такие системы также нельзя назвать идеальными. Несмотря на то, что снимок делается практически мгновенно, пользователю необходимо занять правильное положение по отношению к считывающему устройству таким образом, чтобы расстояние до глаз составляло определённую величину. Это значение может быть различным для разных устройств, но в общем случае составляет несколько десятков сантиметров.

Кроме того, как и любой другой физиологический признак, изображение радужной оболочки не защищено от копирования и воспроизведения злоумышленником. Достаточно качественное изображение радужной оболочки возможно получить с помощью фотографии, а затем использовать в системе, не предусматривающей физический контроль процедуры проверки.

Рукописная подпись

Рукописная подпись — один из классических способов проверки личности, применяемый уже несколько столетий в юридической практике, банковском деле и торговле. Относительно долгая история использования подписи обеспечивает лояльность со стороны общества к этому биометрическому параметру.

Существует два подхода к использованию подписи:

1. Статический, при котором сравниваются изображения подписей. Он является классическим и выполняется человеком на протяжении нескольких столетий.

2. Динамический, при котором используются сведения о колебаниях пишущего пера, силе нажатия, наклоне пера как функции времени [12]. Данный современный подход возможен исключительно для использования компьютерными системами.

Для получения информации о биометрических характеристиках подписи при динамическом подходе всеми современными системами используются графические планшеты (дигитайзеры). Стоимость такого устройства зависит от его характеристик и начинается приблизительно от 100$. Более дорогие дигитайзеры позволяют получать больше признаков, например, угол наклона пера относительно планшета.

Удобство использования подписи варьируется в зависимости от того, как часто человек использует её в повседневной жизни. Люди, привыкшие подписывать десятки документов в день не испытывают какого-либо дискомфорта от данной процедуры. Время её совершения также может быть различным, но в общем случае можно говорить о том, что оно составляет несколько секунд и не существенно отличается от времени ввода пароля с использованием клавиатуры. Недостатком является то, что в существующих системах, применяющих динамический подход, пользователю приходится расписываться пером графического планшета, которое достаточно сильно отличается от привычной авторучки.

Большим преимуществом является то, что при использовании динамического подхода злоумышленник не может скопировать подпись, за исключением случаев, когда информация о динамике воспроизведения передаётся по незащищённым каналам связи. Повторить подпись с теми же характеристиками невозможно даже в том случае, если злоумышленник неоднократно наблюдал процесс её воспроизведения.

Уникальность использования подписи в качестве биометрического аутентификатора заключается в возможности смены аутентификатора по желанию пользователя. Это полезно, если она все же будет каким-либо образом скомпрометирована. Таким образом, подпись можно рассматривать как гибрид подходов с использованием знаний и биометрических характеристик.

Голос

Идентификация человека по голосу также является одним из традиционных способов распознавания, применяемым повсеместно. Можно легко узнать собеседника по телефону, даже не видя его.

Использование голоса является одним из наиболее удобных для пользователя методов. Произнесение требуемой фразы не требует непосредственного контакта пользователя с каким-либо элементом системы. Встроенные устройства звукозаписи присутствуют практически во всех моделях ноутбуков и других

цифровых устройств. Внешний микрофон для персонального компьютера имеет стоимость в несколько долларов США. В целом можно говорить о том, что по стоимости и удобству данный метод определённо можно назвать наиболее привлекательным.

Несмотря на данные преимущества, голосовые методы обладают невысокой надёжностью. Негативно на ней сказывается ещё и то, что голос меняется с возрастом, а также при различных заболеваниях и нарушениях в организме.

Как и в случае с подписью, применение голосового метода в реальной системе не является чисто биометрическим. Пользователю также необходимо знать парольную фразу. Однако в отличие от случая с подписью, в данном методе это является существенным минусом, поскольку злоумышленник может легко подслушать её во время процедуры. Более того не существует особых преград для того, чтобы записать и в дальнейшем использовать реальную голосовую запись для получения несанкционированного доступа. Таким образом, можно говорить о том, что использование голоса возможно в современных биометрических системах исключительно в роли идентификатора.

Заключение

Большинство физиологических биометрических признаков не может получить широкое применение, в первую очередь, по причине нежелания большей части пользователей компьютерных систем передавать в базы данных свои уникальные и неизменяемые параметры. Ситуация обостряется тем, что при их утечке и попаданию к злоумышленнику пользователь не сможет их изменить.

Физиологические параметры, к использованию которых общество относится терпимо, например, изображение лица, не могут обеспечить надёжность распознавания, достаточную для того, чтобы заменить традиционные методы с использованием знаний и собственности. Их применение в системах аутентификации возможно только в роли идентификатора при условии применения программно-аппаратных средств, обеспечивающих быструю и не требующую дополнительных действий со стороны пользователя идентификацию в совокупности с невысокой стоимостью.

В то же время огромные перспективы использования в качестве аутентификатора имеют поведенческие параметры, в частности, рукописная подпись. Несмотря на многочисленные преимущества, данный метод все ещё не получил широкого распространения по причинам, рассмотренным в основной части статьи. Можно выделить следующие направления, в которых необходимо вести работу для того, чтобы подпись стала реальной заменой аутентификации с использованием пароля:

1. Разработка недорогих специализированных аппаратных средств для получения образцов рукописной подписи.

2. Разработка быстрых и надёжных алгоритмов экстракции и сравнения биометрических характеристик рукописной подписи.

3. Разработка удобных для пользователя аутентификационных протоколов с возможностью использования в качестве идентификатора других биометрических признаков.

Литература

1. ФСТЭК России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. URL: http://www.fstec.ru/_docs/doc_3_3_002.htm (дата обращения: 29.06.2012).
2. Утечки корпоративной информации и персональных данных в 2010 году. URL: http://www.anti-malware.ru/node/3632 (дата обращения: 26.08.2012).
3. Что реально угрожает персональным данным? URL: http://www.anti-malware.ru/personal_data_leaks (дата обращения: 26.08.2012).
4. Benjamin Miller Vital signs of identity // IEEE Spectrum. 1994. N. 2. C. 22–30.
5. Rutoken. Российское средство аутентификации. URL: http://www.rutoken.ru/ (дата обращения: 26.08.2012).
6. Болл Р.М. Руководство по биометрии. М. : Техносфера, 2007. 368 с.
7. Сканеры отпечатков пальцев. Классификация и способы реализации. URL: http://habrahabr.ru/post/116458/ (дата обращения: 30.08.2012).
8. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. СПб. : Политехника, 2001. 240 с.
9. PalmSecure Palm Vein Sensor. URL: http://www.amazon.com/PalmSecure-Palm-Vein-Sensor-biometric/dp/B007Y7YU12 (дата обращения: 02.09.2012).
10. Современные биометрические методы идентификации. URL: http://habrahabr.ru/post/126144/ (дата обращения: 02.09.2012).
11. Технологии распознавания радужной оболочки глаза в аэропортах (По материалам доклада «Биометрия в авиационной безопасности», подготовленного для конференции ITE&AIA) // Системы безопасности. 2006. № 5. С. 140–144.
12. Ложников П.С., Еременко А.В. Идентификация личности по рукописным паролям // Мир измерений. 2009. № 4. С. 1–13.

СВЕДЕНИЯ ОБ АВТОРАХ

Багма Александр Владимирович – аспирант, кафедра кибернетики, ОмГУ им. Ф.М. Достоевского.

Вильховский Даниил Эдуардович – студент, факультет компьютерных наук, ОмГУ им. Ф.М. Достоевского.

Гринь Анатолий Гаврилович – д.ф.-м.н., профессор, кафедра кибернетики, ОмГУ им. Ф.М. Достоевского.

Гуц Александр Константинович – д.ф.-м.н., профессор, зав. каф. кибернетики, ОмГУ им. Ф.М. Достоевского.

Ефимов Сергей Сергеевич – к.т.н., доцент, кафедра вычислительных систем, ОмГУ им. Ф.М. Достоевского.

Кошелева Ольга – к.ф.-м.н, доцент, педагогический факультет, Техасский университет в Эль-Пасо, США.

Крейнович Владик – к.ф.-м.н, профессор, факультет компьютерных наук, Техасский университет в Эль-Пасо, США.

Кутателадзе Семён Самсонович – д.ф.-м.н., профессор, главный научный сотрудник Института математики СО РАН им. С.Л. Соболева.

Лонгпре Люк – к.н. по компьютерным наукам, профессор, факультет компьютерных наук, Техасский университет в Эль-Пасо, США.

Лысак Антон Борисович – аспирант, кафедра компьютерных технологий и сетей, ОмГУ им. Ф.М. Достоевского.

Макаренко Александр Владимирович – студент, факультет компьютерных наук, ОмГУ им. Ф.М. Достоевского.

Ортис Андре – студент, Техасский университет в Эль-Пасо, США.

Пугин Константин Витальевич – студент, факультет компьютерных наук, ОмГУ им. Ф.М. Достоевского.

Пыхтеев Александр Викторович – студент, факультет компьютерных наук, ОмГУ им. Ф.М. Достоевского.

Степанов Владимир Николаевич – к.ф.-м.н., доцент, кафедра высшей математики, Омский государственный технический университет.

Стопкин Сергей Викторович – студент, факультет компьютерных наук, ОмГУ им. Ф.М. Достоевского.

AUTHORS

Alexander V. Bagma – Post-graduate Student, Cybernetics Chair, Omsk State University n.a. F.M. Dostoevskiy.

Sergey S. Efimov – Ph.D.(Eng.), Associate Professor, Computational Systems Chair, Omsk State University n.a. F.M. Dostoevskiy.

Anatoly G. Grin – Doctor of Mathematics, Professor, Cybernetics Chair, Omsk State University n.a. F.M. Dostoevskiy.

Alexander K. Guts – Doctor of Mathematics, Professor, Head of Cybernetics Chair, Omsk State University n.a. F.M. Dostoevskiy.

Olga Kosheleva – Ph.D.(Math.), Associate Professor, University of Texas at El Paso, El Paso, TX 79968, USA.

Vladik Kreinovich – Ph.D.(Math.), Professor, Computer Science Department, University of Texas at El Paso, El Paso, TX 79968, USA.

Semen S. Kutateladze – Doctor of Mathematics, Professor, Sobolev Institute of Mathematics.

Luc Longpré – Ph.D. (Computer Science), Professor, Computer Science Department, University of Texas at El Paso, El Paso, TX 79968, USA.

Anton B. Lysak – Post-graduate Student, Computer Technology and Networks Chair, Omsk State University n.a. F.M. Dostoevskiy.

Alexander V. Makarenko – Student, Faculty of Computer Sciences, Omsk State University n.a. F.M. Dostoevskiy.

Andres Ortiz – Undergraduate, Mathematics, University of Texas at El Paso, El Paso, TX 79968, USA.

Konstantin V. Pugin – Student, Faculty of Computer Sciences, Omsk State University n.a. F.M. Dostoevskiy.

Alexander V. Pykhteyev – Student, Faculty of Computer Sciences, Omsk State University n.a. F.M. Dostoevskiy.

Vladimir N. Stepanov – Ph.D.(Math.), Associate Professor, Omsk State Technical University.

Sergey V. Stopkin – Student, Faculty of Computer Sciences, Omsk State University n.a. F.M. Dostoevskiy.

Daniel E. Vilkhovskiy – Student, Faculty of Computer Sciences, Omsk State University n.a. F.M. Dostoevskiy.

АННОТАЦИИ

А.Г. Гринь. О точности нормальной аппроксимации распределений сумм зависимых случайных величин.
Аннотация. Получены оценки скорости сходимости в предельных теоремах о сходимости к нормальному закону для последовательностей слабо зависимых случайных величин без предположения о существовании дисперсии.
Ключевые слова: предельные теоремы, скорость сходимости к нормальному закону, условие равномерно сильного перемешивания.

С.С. Кутателадзе. Дело Лузина — трагедия математики России.
Аннотация. Краткий обзор роли математиков в так называемом «деле академика Лузина» и анализ некоторых математических и гуманитарных корней этого исторического события.
Ключевые слова: академик Н.Н. Лузин, ученики, чрезвычайная Комиссия Академии наук СССР.

В.Н. Степанов. Уравнение первого рода относительно меры на сфере S^{n-1}.
Аннотация. Исследуются свойства интегрального оператора с ядром, зависящим от скалярного произведения и действующего на банаховом пространстве мер на сфере.
Ключевые слова: интегральное преобразование, геометрическая томография, оператор, компактность, мера.

Л. Лонгпре, О. Кошелева. Об однозначных физических определениях случайных и типичных объектов.
Аннотация. Чтобы различать случайные и неслучайные последовательности, Колмогоров и Мартин-Лёф предложили новое определение случайности, согласно которому объект (например, последовательность нулей и единиц) случаен, если он удовлетворяет всем вероятностным законам, т.е., более точно, если он не принадлежит ни одному определимому множеству вероятностной меры 0. Это определение отражает обычную физическую идею о том, что события с вероятностью 0 не могут произойти. Специалисты в области физики — особенно статистической — часто используют более сильное утверждение: события с очень маленькой вероятностью также не могут произойти. Предложена модификация определения Колмогорова-Мартина-Лёфа, которая охватывает это физическое утверждение. Проблема заключается в том, что в отличии от исходного определения, новое определение случайности неоднозначно определено вероятностной мерой: для одной и той же вероятностной меры можно дать несколько различных определений случайности. В этой статье показано, что, несмотря на невозможность определить, например, единственное множество R случайных объектов, можно определить единственную последовательность R_n таких множеств (единственную в некотором разумном смысле).
Ключевые слова: случайный, типичный, случайность Колмогорова-Мартина-Лёфа, физический смысл случайности.

В. Крейнович, А. Ортис. Если энергия не сохраняется, тогда постоянная Планка больше не постоянная: Теорема.
Аннотация. Чтобы экспериментально проверить состоятельность любой физической теории, нужно сформулировать альтернативную теорию и проверить, будут ли результаты экспериментов согласоваться с оригинальной теорией или с альтернативной. В частности, чтобы проверить, сохраняется ли энергия, необходимо сформулировать тео-

рию, в которой энергия не сохраняется. Формулировка такой теории — нелёгкая задача для квантовой физики, где обычное уравнение Шрёдингера косвенным образом предполагает существование оператора энергии (гамильтониана), чьё значение сохраняется. В данной статье показано, что единственный способ получить согласующуюся квантовую теорию без сохранения энергии — это использовать представление Гейзенберга, в котором операторы, представляющие физические величины, меняются во времени. Доказано, что в этом представлении, энергия сохраняется тогда и только тогда, когда постоянная Планка остаётся постоянной. Таким образом, соответствующий квантовый аналог теории без сохранения энергии — это теория, в которой постоянная Планка может меняться, т.е. будет уже не постоянной, а новым полем.
Ключевые слова: отсутствие сохранения энергии, квантовая физика, постоянная Планка.

А.К. Гуц. Модель смены сознания сна и сознания реальности.
Аннотация. Даётся математическое описание сна, в котором, по мнению Флоренского, наблюдается течение времени в обратном направлении.
Ключевые слова: Флоренский, сон, реальность, время, сознание.

А.В. Багма. Обзор высокопроизводительных вычислительных платформ для графических ускорителей.
Аннотация. В статье рассматриваются основные платформы для высокопроизводительных вычислений на графических ускорителях, их основные особенности и характеристики.
Ключевые слова: CUDA, OpenCL, вычисления.

Д.Э. Вильховский, С.С. Ефимов. Исследование алгоритмов определения изоморфности графов в системах с распределённой и общей памятью.
Аннотация. Задача проверки изоморфности графов часто возникает в химии, экономике, статистике, теоретической физике, математической лингвистике и других областях. Целью проведённого исследования являлся сравнительный анализ эффективности использования инвариантов и параллельных реализаций алгоритмов проверки изоморфности графов.
Ключевые слова: инварианты графа, изоморфность, распределенные вычисления.

А.В. Макаренко, А.В. Пыхтеев, С.С. Ефимов. Параллельная реализация и сравнительный анализ алгоритмов факторизации в системах с распределённой памятью.
Аннотация. В статье рассматриваются наиболее популярные на сегодняшний день алгоритмы факторизации целых чисел, предложена их параллельная реализация в системах с распределённой памятью. Получены сравнительные оценки для каждого метода на различном числе параллельных процессов. Сделаны общие выводы об эффективности использования алгоритмов.
Ключевые слова: факторизация, алгоритмы факторизации, параллельная реализация, сравнительный анализ.

К.В. Пугин, С.С. Ефимов. Генетические алгоритмы с частичной параллелизацией в системах с общей памятью на примере задачи коммивояжёра.
Аннотация. Данная статья является описанием опыта частичной параллелизации генетических алгоритмов для решения задачи коммивояжёра. Приведены примеры возможного кода, а также результаты тестов производительности различных вариантов алгоритма. Произведено сравнение вариантов реализации ГА как между собой, так и

с эталонными вариантами.
Ключевые слова: генетические алгоритмы, параллелизация, задача коммивояжёра, OpenMP, CUDA.

С.В. Стопкин, К.В. Пугин, С.С. Ефимов. Распознавание дорожной разметки на базе Intel OpenCV.
Аннотация. В данной статье производится анализ методов распознавания дорожной разметки, а также приводится простой пример реализованного метода, перспективы развития распознавания разметки при помощи интеграции других методов.
Ключевые слова: дорожная разметка, обработка видео, распознавание, OpenCV.

А.Б. Лысак. Идентификация и аутентификация личности: обзор основных биометрических методов проверки подлинности пользователя компьютерных систем.
Аннотация. В статье рассматриваются основные биометрические методы, применяемые в современных компьютерных системах в целях идентификации и аутентификации пользователя. Приводится базовая классификация методов и описываются сферы их применения и ключевые отличия.
Ключевые слова: безопасность, биометрия, аутентификация, идентификация, статические и динамические методы.

ABSTRACTS

A.G. Grin. On the Accuracy of Normal Approximation of Distributions of Sums of Dependent Random Variables.
Abstract. Estimates of the rate of convergence in the limit theorems on convergence to the normal law without of the existence of the variances obtained in this article
Keywords: limit theorems, the rate of convergence to the normal law, uniformly strong mixing condition.

S.S. Kutateladze. Luzin Affair, the Tragedy of Mathematics in Russia.
Abstract. An overview of the role of mathematicians in the so-called "Academician Luzin affair"and analysis of some mathematical and humanitarian roots of this historic event
Keywords: Academician N.N. Luzin, students, special hearing of the Commission of the Academy of Sciences of the USSR.

V.N. Stepanov. Equation of the First Kind for Measures on Sphere S^{n-1}.
Abstract. The characteristic of the integral operator are researched with kernel, depending on inner product and acting on Banach space measures on sphere.
Keywords: integral transformation, geometric tomography, operator, compactness, measure.

L. Longpré, O. Kosheleva. Towards Unique Physically Meaningful Definitions of Random and Typical Objects.
Abstract. To distinguish between random and non-random sequence, Kolmogorov and Martin-Löf proposed a new definition of randomness, according to which an object (e.g., a sequence of 0s and 1s) is random if it satisfies all probability laws, i.e., in more precise terms, if it does not belong to any definable set of probability measure 0. This definition reflect the usual physicists' idea that events with probability 0 cannot happen. Physicists – especially in statistical physics – often claim a stronger statement: that events with a

very small probability cannot happen either. A modification of Kolmogorov-Martin-Löf's (KLM) definition has been proposed to capture this physicists' claim. The problem is that, in contrast to the original KLM definition, the resulting definition of randomness is not uniquely determined by the probability measure: for the same probability measure, we can have several different definitions of randomness. In this paper, we show that while it is not possible to define, e.g., a unique *set* $\mathcal{R}$ of random objects, we can define a unique *sequence* $\mathcal{R}_n$ of such sets (unique in some reasonable sense).
Keywords: random, typical, Kolmorovo-Martin-Löf randomness, physical meaning of randomness.

V. Kreinovich, A. Ortiz. If Energy Is Not Preserved, Then Planck's Constant Is No Longer a Constant: A Theorem.
Abstract. For any physical theory, to experimentally check its validity, we need to formulate an alternative theory and check whether the experimental results are consistent with the original theory or with an alternative theory. In particular, to check whether energy is preserved, it is necessary to formulate an alternative theory in which energy is not preserved. Formulating such a theory is not an easy task in quantum physics, where the usual Schroedinger equation implicitly assumes the existence of an energy (Hamiltonian) operator whose value is preserved. In this paper, we show that the only way to get a consistent quantum theory with energy non-conservation is to use Heisenberg representation in which operators representing physical quantities change in time. We prove that in this representation, energy is preserved if and only if Planck's constant remains a constant. Thus, an appropriate quantum analogue of a theory with non-preserved energy is a theory in which Planck's constant can change – i.e., is no longer a constant, but a new field.
Keywords: energy non-conservation, quantum physics, Planck's constant.

A.K. Guts. Model of Change of Consciousness of a Dream and Reality Consciousness.
Abstract. The mathematical description of a dream, in which, on to the Florensky's opinion, it is observed a time, that moves in the opposite direction.
Keywords: Florensky, dream, reality, time, consciousness.

A.V. Bagma. An Overview of High Performance Computing Platforms for Graphics Cards.
Abstract. This article considers the main platforms for high performance computing on graphics accelerators, their main features and characteristics.
Keywords: CUDA, OpenCl, computing.

D.E. Vilkhovskiy, S.S. Efimov. The Research on Graph Isomorphism Algorithms in Distributed and Shared Memory Systems.
Abstract. The determination of the graph isomorphism appears to be a subject of research in chemistry, economics, statistics, theoretical physics, mathematical linguistics and other scientific fields. The purpose of the research is a comparative analysis of the effectiveness of invariants and parallel realization of algorithm on graph isomorphism.
Keywords: invariants of the graph, isomorphism.

A.V. Makarenko, A.V. Pykhteyev, S.S. Efimov. Parallel Implementation and Comparative Analysis of Factorisation Algorithms in Systems with Distributed Memory.
Abstract. Our paper contains a research of the most popular integer factorisation algorithms and proposes some ways to make their parallel implementation in systems

with distributed memory. We obtain comparative estimates for each method with different number of parallel processes and make general conclusions about their performance
Keywords: factorisation, factorisation algorithms, parallel implementation, comparative analysis.

K.V. Pugin, S.S. Efimov. Studying Partial Parallelized Genetic Algorithms by Solving TSP in Shared Memory Systems.
Abstract. This article is a description of experiment of solving TSP by partial parallelized genetic algorithms in dual-core computer. There are examples of code, results of performance and accuracy tests of different variants of this algorithm. Realizations compared among themselves and with reference non-genetic algorithms
Keywords: genetic algorithms, parallelization, traveling salesman problem, OpenMP, CUDA, Thrust.

S.V. Stopkin, K.V. Pugin, S.S. Efimov. Lane Detecting using OpenCV.
Abstract. There are several lane detecting methods. Some are simple, some are advanced. This article is overview of methods and description of fast realization of one.
Keywords: OpenCV, Video processing, lane detecting, Intel.

A.B. Lysak. Identification and Authentication. Common Biometric Methods Review.
Abstract. Major biometric methods used for identification and authentication purposes in modern computing systems are considered in the article. Basic classification, application areas and key differences are given.
Keywords: computing systems security, biometry, authentication, identification.

Научный журнал

Математические структуры и моделирование

Выпуск 26

Главный редактор
Д.Н. Лавров

Корректор
И.Н. Баловнева

Художественное оформление
В.В. Коробицын

Адрес научной редакции
Россия, 644053, Омск-53, ул. Грозненская, 11
Омский государственный университет
факультет компьютерных наук
E-mail: lavrov@omsu.ru
Электронная версия журнала:
http://msm.univer.omsk.su

Подписано в печать 01.11.12. Формат 60 × 80 1/8.
Усл. печ. л. 16,5. Тираж 100 экз. Заказ № 389.

Отпечатано на полиграфической базе издательства ОмГУ им. Ф.М. Достоевского
644077, г. Омск, пр. Мира, 55А

ISSN 2222-8772