УДК 519.6:519.21

Н.М. ГЛАЗУНОВ

АРИФМЕТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СЛУЧАЙНЫХ ПРОЦЕССОВ И *r*-АЛГОРИТМЫ

Ключевые слова: *недифференцируемая оптимизация, стохастическая аппроксимация случайного процесса, равнораспределенность с заданной плотностью, r-алгоритм, матричная оптимизация.*

ВВЕДЕНИЕ

В работах по оптимизации академик Н.З. Шор наряду с исследованием детерминированных методов недифференцируемой оптимизации, в том числе *r*-алгоритмов, интересовался и разрабатывал с коллегами также методы стохастической оптимизации [1, 2]. Обзор основополагающих публикаций по оптимизации вместе с библиографиями работ до 2000 года представлен в статьях [3, 4]. Исследования академиков И.Н. Коваленко [5], Б.Н. Пшеничного [6], чл.-корр. НАНУ М.В. Михалевича [7], их учеников и коллег составляют фундамент киевской школы теории оптимизации, заложенный учеными Института кибернетики им. В.М. Глушкова НАН Украины.

Данная статья является продолжением работы [8], в которой рассмотрены экономные методы генерации псевдослучайных последовательностей, основанные на арифметических принципах [9]. Эти методы применяются при реализации, а также и при теоретических исследованиях методов стохастической аппроксимации случайных процессов, которые, в свою очередь, служат основой прямых методов стохастической оптимизации. Развивая направления работы [8], мы приводим три класса методов генерации псевдослучайных последовательностей, основанные на арифметических принципах [9, с. 190–266]. Для краткости методы генерации псевдослучайных последовательностей, основанные на арифметических принципах, мы называем процессами. Ниже рассматриваются процессы Сато–Тэйта, Клостермана и Линника–Кубилюса.

Н.З. Шор ввел и разработал с коллегами понятие *r*-алгоритма [10]. При этом он обращал внимание на необходимость исследования применимости *r*-алгоритмов к новым классам задач с возможным при этом расширением понятия *r*-алгоритма, например задачам матричной оптимизации, которые в большинстве являются задачами недифференцируемой минимизации. В статье исследуется класс задач матричной недифференцируемой оптимизации, связанный с проблемой заполнения матрицы по выборке ее элементов с условием минимизации некоторой функции от матрицы. Задача восстановления матрицы по выборке ее элементов формулируется как задача выпуклой оптимизации. Для ее решения предлагается применение *r*-алгоритмов. Представлена общая схема. Задача восстановления матрицы по выборке ее элементов возникает во многих математических и прикладных исследованиях. Назовем следующие прикладные задачи: базы данных; триангуляция по неполным данным; сжимаемое опознавание (Compressed Sensing); машинное обучение (Machine Learning).

Базы данных. Пусть в матрице M (таблице) строки соответствуют пользователям, а столбцы — вопросам. Данные накапливаются в этой таблице, но обычно многие вопросы остаются без ответа. Можно ли с той или иной степенью точности восстановить опущенные ответы?

Триангуляция по неполным данным. Имеется частичная информация о расстояниях между точками некоторой ограниченной области. Можно ли восстановить геометрию области по этим неполным данным? Здесь матрица ранга 2, если область на плоскости, и ранга 3, если область в пространстве.

Машинное обучение — процесс отображения данных низкого уровня в другие форматы, в которых эти данные могут быть более компактными, более абстрактными или более полезными. Сжимаемое опознавание рассмотрено ниже.

Одна из математических формулировок перечисленных выше задач имеет следующее представление:

$$\min \operatorname{rank}(X) \text{ при } X_{ij} = M_{ij}(i,j) \in \Omega,$$

где X — искомая матрица размера $n_1 \times n_2$, M_{ij} — наблюдаемые значения элементов матрицы в выборке номеров строк и столбцов $(i,j) \in \Omega$ ее элементов. К сожалению, как доказано в [11], в такой постановке задача суперэкспоненциальна по сложности. Пусть X^* — матрица, сопряженная к X. Известно, что ненулевые собственные значения матриц XX^* и X^*X совпадают и положительны.

Арифметические значения квадратных корней из общих собственных значений матриц XX^* и X^*X называют сингулярными значениями матрицы X. Далее полагаем, что σ_k есть k-е сингулярное значение матрицы X и что эти сингулярные значения занумерованы в порядке убывания $\sigma_1 \ge \sigma_2 \ge \ldots \ge \sigma_n > 0$, где σ_n — наименьшее сингулярное значение. Сингулярные значения $\sigma_{n+1} \ldots$ полагают нулевыми.

Определение. Ядерной нормой матрицы X называют величину $||X||_* = \sum_{k=1}^{n} \sigma_k(X)$, где $\sigma_k(X)$ есть k-е сингулярное значение X. В работе [28] предложено исследовать задачу (с ядерной нормой): $\min ||X||_*$ при $X_{ij} = M_{ij}(i,j) \in \Omega$.

Использование сингулярного разложения матрицы X позволяет рассматривать эту задаче как задачу полуопределенного программирования [1]. Для ее решения, следуя [1], предлагается матричное расширение r-алгоритма Н.З. Шора. Относительно r-алгоритмов о результатах работы предварительно докладывали на конференции в Институте кибернетики им. В.М. Глушкова, посвященной 50-летию теории и практике r-алгоритмов. Пользуясь случаем, автор выражает признательность П.И. Стецюку за приглашение принять участие и выступить с докладом, а также всем участникам за обсуждение и полезные замечания.

ПРОЦЕССЫ ТИПА САТО–ТЭЙТА

Пусть $E: y^2 = x^3 + ax + b,\ a, b \in Z$ — эллиптическая кривая над кольцом целых чисел $\mathbb{Z}$. Вне конечного множества простых, являющихся делителями дискриминанта, кривая E имеет хорошую редукцию в простом конечном поле $\mathbf{F}_p$. Число точек $\# E(\mathbf{F}_p)$ проективного замыкания кривой E при локализации по $\bmod p$ выражается формулой $\# E_p = 1 + p - a_p$, где $a_p = 2\sqrt{p}\cos\varphi_p$, а сама кривая E рассматривается как проективная. Гипотеза Сато–Тэйта [12] утверждает, что для эллиптической кривой без комплексных умножений углы φ_p, соответствующие a_p, равно распределены на интервале $[0,\pi)$ с плотностью $(2/\pi)\sin^2 t$. Иногда рассматривают нормализованное значение $a_p^{\text{norm}} = \dfrac{1}{2\sqrt{p}} a_p$, которое принадлежит интервалу $[-1,1]$, $a_p^{\text{norm}} = \cos\varphi_p$. В этом случае гипотеза Сато–Тэйта эквивалентна утверждению, что a_p^{norm} равно распределены на $[-1,1]$ с ве-

роятностной мерой плотности $\frac{2}{\pi}\sqrt{1-t^2}$. Рассмотрим процессы Берча, процессы Иошиды [14], процессы Сато–Тэйта по Клозелю–Харрису–Шеффердю–Барону–Тэйлору (Clozel, Harris, Shepherd-Barron, Taylor), которые недавно получили при некоторых условиях доказательство гипотезы Сато–Тэйта [15, 16].

Процессы Берча. Б. Берч рассмотрел ситуацию, когда эллиптическая кривая над $\mathbf{F}_p$ при $p \geq 5$ задана уравнением $zy^2 = x^3 + axz + bz^3$. Выбирая возрастающую последовательность простых, стремящуюся к бесконечности, для каждого простого p из этой последовательности рассматривается множество кривых указанного вида, имеющих $1 + p - a_p$ точек в $\mathbf{F}_p$. Используя моменты, соответствующие $\sin^2$-распределению, а также операторы Гекке, действующие на пространстве параболических форм, соответствующих эллиптическим кривым, доказано, что аналог гипотезы Сато–Тэйта в рассматриваемой ситуации истинен (подробности в [13]).

Процессы Иошиды. Х. Иошида рассмотрел аналог гипотезы Сато–Тэйта при редукции эллиптических кривых для любых простых p в случае рассмотрения множества эллиптических кривых над полем $\mathbf{F}_{p^m}$. Каждая такая эллиптическая кривая однозначно определяется своим модулярным инвариантом $j \in \mathbf{F}_{p^m}$. Рассматривая эллиптические кривые с $j \in \mathbf{F}_{p^m} - \{0,1\}$, Иошида получает для множеств углов $S_m = \{\varphi_j, -\varphi_j, \pi - \varphi_j, \varphi_j - \pi\}$ утверждение, что для последовательности $\{S_m\}_{m=1}^{\infty}$ функция плотности есть $\pi^{-1}(\sin\varphi)^2$, т.е. доказательство аналога гипотезы Сато–Тэйта [14].

Процессы Сато–Тэйта. Пусть E — эллиптическая кривая без комплексных умножений над полем рациональных чисел $\mathbb{Q}$. Известная гипотеза Ланглендса [17] в случае эллиптических кривых утверждает, что некоторые симметрические степени L-функций продолжаются до целых функций и совпадают с некоторыми L-функциями.

Теорема 1 (Клозел–Харрис–Шефферд-Баррон–Тэйлор). Пусть E — эллиптическая кривая над $\mathbb{Q}$ с нецелым j-инвариантом. Тогда для всех $n > 0$ функция $L(s, E, \mathrm{Sym}^n)$ продолжается до мероморфной функции, которая является голоморфной и не обращающейся в ноль при $\mathrm{Re}\, s \geq 1 + n/2$.

Этих условий достаточно для доказательства гипотезы Сато–Тэйта.

Таким образом, взяв эллиптическую кривую, удовлетворяющую условиям теоремы, и выбрав возрастающую до бесконечности последовательность простых чисел без простых, делящих дискриминант кривой E (напомним, что простых делителей дискриминанта — конечное число), в соответствии с доказанной в приведенных выше условиях гипотезой Сато–Тэйта получим равномерно распределенную с плотностью $\pi^{-1}(\sin\varphi)^2$ последовательность углов φ_p.

ПРОЦЕССЫ ТИПА КЛОСТЕРМАНА

Рассмотрим

$$y^p - y = cx + d/x, \quad c, d \in \mathbf{Z},\ c, d \text{ не сравнимы с } 0 \pmod p, \tag{1}$$

накрытие Артина–Шрайера [18] над полем $\mathbf{F}_{p^r}$ $(r \geq 1)$ — конечным расширением поля $\mathbf{F}_p$.

Пусть

$$f(t) = t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n \tag{2}$$

— многочлен из $\mathbf{F}_{p^r}[t]$ с $a_n \neq 0$ в $\mathbf{F}_p$. В некотором конечном расширении k поля

$\mathbf{F}_p$ имеет место разложение $f(t) = (t-\alpha_1)\dots(t-\alpha_n)$. Положим $l(f) = c(\alpha_1 + \dots + \alpha_n) + d(1/\alpha_1 + \dots + 1/\alpha_n)$, где $\alpha_1, \dots, \alpha_n$ — корни (2). Для многочленов вида (2) имеет место

$$l(f_1 f_2) = l(f_1) + l(f_2). \tag{3}$$

Пусть $\mathrm{tr}: \mathbf{F}_{p^r} \to \mathbf{F}_p$ — отображение следа. Тогда в условиях выполнения (3) $\mathrm{Tr}(l(f_1 f_2)) = \mathrm{Tr}(l(f_1)) + \mathrm{Tr}(l(f_2))$.

Для заданного многочлена вида (2) определим по аналогии с [9, с. 18–25] характер $\chi(f) = e^{2\pi i \nu Tr(l(f))/p}$, где ν — одно из чисел множества $0, 1, 2, \dots, p-1$, $\chi(f) = 0$, если $a_n = 0$ в $\mathbf{F}_p$.

Легко проверить, что $\chi(f_1 f_2) = \chi(f_1)\chi(f_2)$.

Для накрытия вида (1) над F_{p^r} L-функцию определяют равенством

$$L(z, \chi) = \prod_{m=1}^{\infty} \prod_{p(t)} \frac{1}{(1 - \chi(p(t)) z^m)}, \tag{4}$$

где внутреннее произведение распространяется на все неприводимые в $\mathbf{F}_{p^r}[t]$ многочлены со старшим коэффициентом 1, $\nu \geq 1$. При $\nu = 0$ функция $L(z, \chi_0) = (1 - p^r z)^{-1}$.

Положим $T_r(\nu; c, d) = \sum_{\xi} e^{2\pi i \nu \frac{\mathrm{Tr}(c\xi + d/\xi)}{p}}$, $\nu = 0, 1, 2, \dots, p-1$, ξ пробегает элементы мультипликативной группы поля $\mathbf{F}_{p^r}$, $T_p(c, d) = \sum_{x=1}^{p-1} e^{2\pi i \frac{cx + d/x}{p}}$ (сумма Клостермана).

Замечание 1. $T_1(\nu; c, d) = T_p(c, d)$ при $\nu = 0, 1, 2, \dots, p-1$.

Теорема 2. Произведение (4) сходится при $|z| < 1/p^r$. Функция (4) является многочленом второй степени и имеет вид $L(z, \chi_\nu) = 1 + T_r(\nu; c, d) z + p^r z^2$.

Доказательство теоремы приведено в [19].

Положим

$$W_p(z) = \prod_{\nu=1}^{p-1} L_p. \tag{5}$$

Теорема 3. Корни (5) имеют абсолютную величину, равную $1/\sqrt{p}$.

Доказательство теоремы может быть получено на основе оценок А. Вейля [20] или метода С.А. Степанова [21] и приведено в [19].

Следствие 1. $T_p(c, d) = 2\sqrt{p} \cos \theta(c, d)$.

Автор исследовоал распределение углов θ_p сумм Клостермана на интервале $[0, \pi]$ в следующих двух случаях.

1. Доказанный Н. Кацем [22] и А. Адольфсоном [23] случай распределения углов сумм Клостермана

$$T_p(c, d) = \sum_{x=1}^{p-1} e^{2\pi i \frac{cx + d/x}{p}}$$

с функцией плотности $(2/\pi)\sin^2 t$ в случае, когда c, d независимо пробегают $\mathbf{F}_p$, cd не делится на p, а p стремится к бесконечности.

2. Проверка гипотезы для суммы $T_p(c,d)=\sum_{x=1}^{p-1} e^{2\pi i\frac{(cx+d/x)}{p}}$, $c=d=1$, на выборке из 1600 последовательных простых, когда сумма фиксирована (фиксированы параметры c и d).

Проведено сопоставление результатов компьютерных вычислений теперь уже известного случая 1 и предполагаемого, но не доказанного к настоящему времени гипотетического распределения для случая 2.

МЕТОДИКА ВЫЧИСЛЕНИЙ И ИХ ОБРАБОТКА

В процессе счета для каждого простого p вычислялись значения T_p, $\cos\theta_p$, θ_p. Запишем примеры абсолютных значений $\cos\theta_p$ сумм Костермана T_p для различных простых p (табл. 1).

Таблица 1. Абсолютные значения $\cos\theta_p$

Большие значения	p	2	7	29	103	1549	3041	5059	7537	10181	13171
	$\cos\theta_p$	,35355	,38721	,47823	,52564	,66391	,75232	,78164	,85773	,95269	,96537
Малые значения	p	2	41	97	383	487	709	1613	2161	3719	10889
	$\cos\theta_p$	,35355	,31430	,10634	,08503	,05637	,04543	,03436	,02577	,01499	,00499

Интервал $[0,\pi]$ разбиваем на 20 подынтервалов: $U_i=\left[\frac{(i-1)\pi}{20},\frac{i\pi}{20}\right]$, $i=1,2,\ldots,20$, i — номер интервала U_i, $\nu(U_i)$ — количество углов θ_j (где j: $1\le j\le n$, — номер последовательного простого), попавших в интервал U_i, $h(U_i)$ — гипотетическое количество углов θ_j, содержащихся в интервале U_i для данной выборки при $\sin^2 t$ распределении, $p_i=\frac{2}{\pi}\int \sin^2 t dt$, $h(U_i)=||np_i||$, где $||\alpha||$ — ближайшее целое к α, n — число элементов в выборке.

Случай А. Вычисления и теория показывают, что распределение значений углов $\theta_p(c,d)$ сумм $T_p(c,d)=\sum_{x=1}^{p-1} e^{2\pi i\frac{(cx+d/x)}{p}}$ по интервалам $U_i=\left[\frac{(i-1)\pi}{20},\frac{i\pi}{20}\right]$, $i=1,2,\ldots,20$, при $c=\text{const}$, $1\le d\le p-1$, одинаково при различных $1\le c\le p-1$. Ввиду этого далее приводятся экспериментальные данные распределения углов сумм $T_p(c,d)$ при $c=\text{const}, 1\le d\le p-1$. Так, для $p=1597$, $c=890, 1\le d\le p-1$ результаты вычислений суммируются в табл. 2, обозначения описаны выше.

Подсчитаем теперь по χ^2 — критерию Пирсона [24], вероятность отвергнуть гипотезу о $\sin^2 t$ распределении, используя данные таблицы. Поскольку в каждый интервал должно попадать не меньше десяти значений, объединяем интервалы U_1, U_2 и U_3 и интервалы U_{19} и U_{20}.

Утверждение 1. В случае А для табл. 2 с 16-ю степенями свободы $\chi^2=7{,}52$.

Случай Б. Результаты вычислений на выборке из 1600 последовательных простых от 2 до 13499 приведены в табл. 3.

Обработка результатов вычислений по χ^2 критерию Пирсона аналогична случаю А). Так как в каждый интервал должно попадать не меньше десяти значений, объединяем интервалы U_1, U_2 и U_3 и интервалы U_{18}, U_{19} и U_{20}.

Утверждение 2. В случае Б с 15-ю степенями свободы $\chi^2=10{,}1806$.

Таблица 2. Экспериментальные данные распределения углов $\theta_p(c,d)$ при $p=1597,\ c=890,\ 1\le d\le p-1$

i	$v(U_i)$	$h(U_i)$	i	$v(U_i)$	$h(U_i)$
1	0	1	11	154	158
2	6	9	12	158	151
3	29	24	13	141	136
4	51	44	14	109	116
5	65	67	15	99	92
6	90	92	16	70	67
7	111	116	17	44	44
8	134	136	18	18	24
9	154	151	19	7	9
10	153	158	20	3	1
Всего	793			803	

Таблица 3. Экспериментальные данные распределения углов для 1600 последовательных простых от 2 до 13499

i	$v(U_i)$	$h(U_i)$	i	$v(U_i)$	$h(U_i)$
1	0	1	11	164	159
2	7	9	12	141	151
3	25	24	13	150	136
4	41	44	14	128	116
5	66	68	15	106	92
6	98	92	16	67	68
7	99	116	17	40	44
8	132	136	18	25	24
9	152	151	19	2	9
10	156	159	20	1	1
Всего	776			824	

Сопоставляя вычисленное значение χ^2 с таблицами для χ^2-распределения, получаем, что гипотеза о равнораспределенности углов θ_p на интервале $[0,\pi]$ с функцией плотности $\left(\frac{2}{\pi}\right)\sin^2 t$ (5-процентный уровень значимости по χ^2-критерию Пирсона) верна.

ПРОЦЕССЫ ТИПА ЛИННИКА–КУБИЛЮСА

Приведем два частных случая конструкций Линника–Кубилюса, используя обозначения из [25, гл. X]. Там же рассматриваются общие случаи. Пусть $N_u\{\ldots\}$ обозначает число натуральных чисел $n\le u$, удовлетворяющих условиям, указанным в скобках.

Процессы Давенпорта–Эрдеша. Пусть p — нечетное простое число, вещественное $h>0$, $(\frac{a}{p})$ — символ Лежандра, m — целое число, $S_p(m,h)=$

$=\frac{1}{\sqrt{h}}\sum_{n\le h}\left(\frac{m+n}{p}\right)$ — нормированные суммы. Давенпорт и Эрдеш в работе [26] показали, что при $p\to\infty$, $h=h_{(p)}\to\infty$, $\log h/\log p\to 0$ суммы $S_p(m;h)$, $1\le m\le p$, распределены асимптотически по нормальному закону

$$\frac{1}{p}N_p\{S_p(m;h)<x\}\to\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{u^2}{2}}du.$$

Процессы Линника–Кубилюса. В [25, гл. X] Линник и Кубилюс рассматривают более общие суммы символов Лежандра (обозначения те же вида $S_p(m,t;h)=\frac{1}{\sqrt{h}}\sum_{n\le ht}\left(\frac{m+n}{p}\right)$), где $t\ge 0$ вещественное, и, обобщая метод работы [26], доказывают, что суммы $S_p(m,t;h)$ представляют собой в пределе броуновское движение. Далее они обобщают этот результат на случай составных p, вводя символ Якоби $\left(\frac{a}{P}\right)$, где $P>1$ — нечетное бесквадратное число, и суммы

$$S_p(m,s,t;h)=\frac{1}{\sqrt{h}}\sum_{hs\le n\le ht}\left(\frac{m+n}{p}\right),\quad 0\le s\le t.$$

В этих обозначениях второй из классов процессов Линника–Кубилюса порождается следующим способом: P пробегает любую возрастающую бесконечную последовательность нечетных бесквадратных чисел такую, что для всякого фиксированного $c\ge 0$, $\prod_{p|P}\left(1-\frac{c}{p}\right)\to 1$ при $P\to\infty$, $h=h(P)\to\infty$, $\log h/\log p\to$ $\to 0$, а выражающееся через $S_p(m,s,t;h)$ приращение сумм $S_p(m,t;h)-$ $-S_p(m,s;h)$, $0\le s<t$, является асимптотически нормальным с параметрами 0, $\sqrt{t-s}$:

$$\frac{1}{p}N_p\{S_p(m;s,t;h)<x\}\to\frac{1}{\sqrt{2\pi(t-s)}}\int_{-\infty}^{x}e^{-\frac{u^2}{2(t-s)}}du,$$

а приращения $S_p(m,t_k;h)-S_p(m,s_k;h)$, $0\le s_k<t_k$ $(k=1,\dots,r)$ — асимптотически независимыми для любого конечного набора непересекающихся интервалов $(s_1,t_1),\dots,(s_r,t_r)$:

$$\left\{\frac{1}{p}N_p\{S_p(m,s_1,t_1;h)<x_1\},\dots,\frac{1}{p}N_p\{S_p(m,s_r,t_r;h)<x_r\}\right\}\to$$
$$\to\prod_{k=1}^{r}\lim_{P\to\infty}\frac{1}{P}N_p\{S_p(m,s_k,t_k;h)<x_k\}$$

СЖИМАЮЩИЕ ВЫБОРОЧНЫЕ МЕТОДЫ И *r*-АЛГОРИТМЫ

Опишем задачу восстановления матрицы по выборке ее элементов как задачу выпуклой оптимизации и метод ее решения матричным *r*-алгоритмом. Задача восстановления матрицы по выборке ее элементов возникает во многих теоретических и прикладных исследованиях [27, 28]. Например, пусть на плоскости или в трехмерном пространстве, в частности на неплоской поверхности, установлены сенсоры, каждый из которых может измерять расстояние до сенсоров, ближайших к нему. Требуется указать все расстояния между установленными сенсорами, т.е. реконструировать геометрию, описывающую их расположение (провести триангуляцию).

Автор впервые столкнулся с подобной задачей при исследовании некоторых задач распознавания, частично представленных в [29].

Приведем определения сжимаемого опознавания (compressed sensing) из работ [28, 30–32]. Сжимаемое опознавание (СО) есть подход, в котором измерение сигнала выполняется посредством небольшого по сравнению с обычными методами числа измерений [30, 31]. Сжимаемое опознавание, или сжатая выборка (compressive sensing) есть новая парадигма добывания информации об представляющем интерес объекте посредством весьма неполного множества измерений [32].

Отметим, что вышеприведенные (и некоторые другие) определения СО связаны с измерениями и сжатием информации. Большинство подходов к СО зависят также от еще одного специфического допущения, которое, как известно, выполняется во мно-

гих задачах обработки сигналов и изображений: это принцип разреженности преобразования [30], что в матричном представлении означает разреженность матриц.

В постановке задачи минимизации и в некоторых методах наряду с работой [1] мы следуем работе [32], в которой проводили вычисления на SDP солвере SDPT3 [33] в рамках системы MATLAB. К сожалению, трудно оценить эффективность методов полуопределенного программирования, реализованных в [33]; более того, затруднительно вообще определить используемые в SDPT3 методы. Напомним, что исследуемая задача недифференцируемая. Действительно, ранг исследуемой матрицы, как и число ее сингулярных значений являются целыми числами, т.е. они — недифференцируемые функции элементов матрицы. Это определяет необходимость применения методов недифференцируемой оптимизации.

Нормы. Для векторов $x, y \in \mathbb{R}^n$ со скалярным произведением (x, y) будем использовать евклидову l_2 норму, которую обозначим $||x|| = \sqrt{(x,x)}$. Для матриц X, Y, X_0 из $\mathbb{R}^{n_1 \times n_2}$ через $(X, Y) = \text{tr}\,(X^* Y)$ обозначаем скалярное произведение в $\mathbb{R}^{n_1 \times n_2}$. Евклидову норму матрицы X обозначаем $||X||_E = (X, X)^{1/2}$. Спектральная норма матрицы X равна наибольшему сингулярному значению матрицы X и обозначается $||X||$. Ядерная норма X есть $||X||_*$.

Замечание 2. Для матрицы $A \in \mathbb{R}^{n_1 \times n_2}$

$$||A||_E = (\text{tr}\ AA^*)^{1/2} = (\text{tr}\ A^* A)^{1/2} = \left(\sum_{i=1}^{n} \sigma_i^2 \right)^{1/2},$$

где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — ненулевые сингулярные значения матрицы A.

Субградиент. Напомним определение субградиента выпуклой функции $f: \mathbb{R}^{n_1 \times n_2} \to \mathbb{R}$.

Определение. Матрица $g_f(X_0)$, удовлетворяющая условию

$$f(X) - f(X_0) \geq (g_f(X_0), X - X_0)$$

для всех $X \in \mathbb{R}^{n_1 \times n_2}$, называется субградиентом f в X_0.

Множество

$$\partial f(X_0) = \{X^* \in \mathbb{R}^{n_1 \times n_2} \mid f(X) - f(X_0) \geq (X^*, X - X_0)\}$$

называют субдифференциалом f в точке X_0.

Пусть $A \otimes B$ — тензорное произведение (произведение Кронекера) двух прямоугольных матриц над полем вещественных чисел. Ниже будем использовать его в основном для векторов.

Замечание 3. Пусть $A \in \mathbb{R}^{n_1 \times n_2}$ — матрица ранга r с сингулярным разложением вида $A = \sum_{1<i<r} \sigma_i u_i \otimes v_i^*$. Тогда субградиент ядерной нормы A известен и имеет представление $g_*(A) = \sum_{1<i<r} u_i \otimes v_i^* + W$. Матрица W удовлетворяет известным свойствам (в частности, $||W|| \leq 1$).

***r*-алгоритм.** Одним из наиболее эффективных методов недифференцируемой оптимизации является метод субградиентного типа с растяжением пространства в направлении разности двух последовательных субградиентов [1]. Ниже представлена схема применения матричных *r*-алгоритмов к задачам сжимаемого опознавания. Мы следуем [1]. Так как $\mathbb{R}^{n_1 \times n_2}$ — евклидово пространство, будем рассматривать элементы $\mathbb{R}^{n_1 \times n_2}$ как элементы евклидова пространства E^n, скалярное произведение в котором обозначаем (,). Оператор растяжения пространства в направлении ξ с коэффициентом растяжения α обозначаем $R_\alpha(\xi)$. Этот

оператор при применении его к элементу x из евклидова пространства E^n растягивает в α раз $(x,\xi)\xi$ и не меняет $x-(x,\xi)\xi$.

Пусть f — выпуклая функция на E^n такая, что $f\to\infty$, когда $||x||\to\infty$, $x_0\in E^n$ — начальное значение и B_0 — неособая $n\times n$-матрица (например, $B_0=I_n$ (единичная матрица)), $h_0>0$ — шаговый множитель. Надлежащий выбор используемых ниже шаговых множителей $h_0,h_1,h_2,\ldots$ и обратных значений коэффициентов растяжения пространства $\beta_1,\beta_2,\ldots$ описан в [1].

Шаг 1. Вычисляем $g_0=g_f(x_0);\overline{g_0}=B_0^Tg_0;\ \xi_0=\dfrac{\overline{g_0}}{||\overline{g_0}||},\ x_1=x_0-h_0B_0\xi.$

После k-го шага получаем $x_k\in E^n$, $g_f(x_{k-1})\in E^n$, B_{k-1} — $n\times n$-матрица.

Шаг $k+1$. Вычисляем

$$g_f(x_k);d_k=g_f(x_k)-g_f(x_{k-1});\quad B_k=B_{k-1}\cdot R_{\beta_k}(\xi_{k-1}),\ 0<\beta_k<1;$$

$$r_k=B_k^Td_k;\ \xi_k=\frac{r_k}{||r_k||};\ \overline{g_k}=B_k^Tg_f(x_k);\quad p_k=\frac{\overline{g_k}}{||\overline{g_k}||};\ x_{k+1}=x_k-h_kB_kp_k,$$

где $h_k>0$ есть k-й шаговый множитель.

Стоп, если выполнен критерий окончания вычислений.

Проектирование. Пусть V — подпространство размерности r в E^n и P_V — ортогональная проекция на V. В процессе вычислений нужно проектировать с применением P_V, а также проектировать точки пространства E^n на замкнутое выпуклое подпространство S из E^n. Задача проектирования точки $\alpha\in E^n$ на S имеет представление

$$d(x)=||x-\alpha||\to\min,\ x\in S,$$

а ее решением есть решение $d(x)=\min||x-\alpha||$, $x\in S$ этой задачи минимизации.

Применение вышеописанной методики к исследованию некоторых задач обработки сигналов и изображений представлено в [34].

Выводы. Продолжая исследования статьи [8], мы представили три класса методов генерации псевдослучайных последовательностей, основанные на арифметических принципах, а именно, процессы Сато–Тэйта, Клостермана и Линника–Кубилюса. Следуя замечанию Н.З. Шора о целесообразности исследования применимости r-алгоритмов к новым классам задач, мы представили основанный на r-алгоритме метод исследования задачи восстановления матрицы по выборке ее элементов.

СПИСОК ЛИТЕРАТУРЫ

1. Shor N.Z. Nondifferentiable optimization and polynomial problems. — Boston: Kluwer Acad. Publ. 1998. — 394 p.
2. Ермольев Ю.М., Шор Н.З. О минимизации недифференцируемых функций // Кибернетика. — 1967. — № 1. — С. 101–102.
3. Михалевич В.С., Сергиенко И.В., Шор Н.З. Исследования методов решения оптимизационных задач и их приложения // Там же. — 1981. — № 100. — С. 89–113.
4. Сергиенко И.В., Шор Н.З. Академик В.С. Михалевич — ученый и организатор науки // Кибернетика и системный анализ. — 2000. — № 1. — С. 77–100.
5. Коваленко И.Н. Вероятностный расчет и оптимизация. — Киев: Наук. думка, 1989. — 260 с.
6. Пшеничный Б.Н. Выпуклый анализ и экстремальные задачи. — М.: Наука, 1980. — 320 с.
7. Михалевич М.В. Методы поиска наиболее предпочтительного элемента на множестве Парето-оптимальных решений // Кибернетика и системный анализ. — 1990. — № 5. — С. 34–37.

8. Глазунов Н.М., Постникова Л.П., Шор Н.З. Арифметическое моделирование случайных процессов и эргодическая теория // Кибернетика и системный анализ. — 2004. — № 4. — С. 73–86.
9. Постников А.Г. Избранные труды. — М.: Физматлит, 2005. — 512 с.
10. Шор Н.З., Журбенко Н.Г. Метод минимизации, использующий операцию растяжения пространства в направлении разности двух последовательных градиентов // Кибернетика. — 1971. — № 3. — С. 51–59.
11. Chistov A.L., Grigoriev D.Yu. Complexity of quantifier elimination in the theory of algebraically closed fields // Proc. of the 11th Sympos. on Mathemat. Foundat. of Comput. Sci. Lecture Notes in Comput. Sci. Vol. 176. (Berlin: Springer, 1984). 1984. — P. 17–31.
12. Серр Ж.-П. Абелевы l-адические представления и эллиптические кривые. М.: Мир, 1972. — 191 с.
13. Birch B. How the number of points of an elliptic curve over a fixed prime field varies // Journ. London Math. Soc. — 1968. — **43**. — P. 57–60.
14. Yoshida H. On an analogue of the Sato conjecture // Inventiones Math. — 1973. — 19. — P. 261–277.
15. Harris M., Shepherd-Barron N., Taylor R. A family of Calabi-Yau varieties and potential automorphy // Annals of Math. — 2010. — **171**. — P. 779–813.
16. Clozel L., Harris M., Taylor R. Automorphy for some *l*-adic lifts of automorphic mod Galois representations // Pub. Math. IHES. — 2008. — **108**. — P. 1–181.
17. Langlands R.F. Problems in the theory of automorphic forms // Lectures Notes in Math. — 170. — Berlin: Springer-Verlag. — 1970. — P. 18–61.
18. Серр Ж.-П. Алгебраические группы и поля классов. — М.: Мир, 1968. — 285 с.
19. Глазунов Н.М. О пространствах модулей, равнораспределенности, оценках и рациональных точках алгебраических кривых // Укр. мат. журн. — 2001. — **53**, № 9. — С. 1174–1183.
20. Weil A. Sur le courbes algebriques // Actualites Sci. Ind. — 1948. — **1041**. — P. 1–85.
21. Степанов С.А. Конструктивный метод в теории уравнений над конечными полями // Тр. Мат. ин-та АН СССР. — 1973. — **132**. — С. 237–246.
22. Katz N.M. Gauss Sums, Kloosterman Sums, and Monodromy Groups. — Princeton: Princeton Univ. Press, 1988. — 186 p.
23. Adolphson A. On the distribution of angles of Kloosterman sums // Journ. fur die reine und angew. Math. — 1989. — **395**. — P. 214–220.
24. Крамер Г. Математические методы статистики. — М.: Мир, 1975. — 475 с.
25. Линник Ю.В. Эргодические свойства алгебраических полей. — Ленинград: Изд-во ЛГУ, 1967. — 208 с.
26. Davenport P., Erdos H. The distribution of quadratic and higher residues // Publ. Math. — 1952. — **2**, N 3–4. — P. 252–265.
27. So A.M., Ye Y. Theory of semidefinite programming for sensor network localization // Math. Program. — 2007. — **109,** N 2. — P. 367–384.
28. Candes E., Romberg J. Sparsity and incoherence in compressive sampling // Inverse Probl. — 2007. — **23**, N 3. — P. 969–985.
29. Глазунов Н.М. Об оценках информативности признаков в задачах классификации I, II // Автоматизация проектирования информационных систем. — Киев: Ин-т кибернетики АН УССР, 1976. — С. 57–78.
30. Donoho D.L. Compressed sensing // IEEE Trans. Inf. Theory. — 2006. — **52**, N 4. — P. 1289–1306.
31. Romberg J., Wakin M. Compressed Sensing: A Tutorial. — http: // users.ece.gatech.edu/justin/ssp2007.
32. Candes E., Recht B. Exact Matrix Completion via Convex Optimization // Found. Comput. Math. — 2009. — **9**. — P. 717–772.
33. Toh K.C., Todd M.J., Tutuncu R.H. SDPT3 — a MATLAB software package for semidefinite-quadratic-linear programming. Available from http://www.math.nus.edu.sg/~m attohkc/sdpt3.html.
34. Glazunov N.M. Compressed sensing and r-algorithms // Proceedings 2011 Microwaves, Radar and Remote Sensing Symposium. 2011. — Kiev: NAU. — P. 139–141.

Поступила 02.08.2011