Согласно предложению 1 и определению функции φ имеем

$$c_\nu = \sum_{\lambda=0}^{p-1} \bar{\varphi}_{\lambda\nu} f_\lambda = \sum_{\lambda=0}^{p-1} \frac{1}{p} \sum_{j=0}^{p-1} e^{-\frac{2\pi i}{p}\alpha j} (r_{-1}, g_{-1})^{-\lambda j} (r_{-1}, g_{-1})^{\nu j} f_\lambda =$$

$$= \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} e^{-\frac{2\pi i}{p}(\alpha j - \nu j)} \sum_{\lambda=0}^{p-1} \frac{1}{\sqrt{p}} e^{-\frac{2\pi i}{p}\lambda j} f_\lambda = \sum_{j=0}^{p-1} \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p} j(\nu-\alpha)} \hat{f}(j) = f_{\nu-\alpha},$$

откуда и следует предложение 2, так как разность $\nu - \alpha$ в $f_{\nu-\alpha}$ понимается как вычитание по $\bmod 2$. $\square$

Замечание. Если ключ κ есть произвольный вектор, принадлежащий множеству $[0, p-1]^p$, то зашифрованное сообщение $C = (c_k)_{k=0}^{p-1}$ не обязано быть перестановкой исходного сообщения. Например, при $p = 11$, $f = (c\,o\,e\,f\,f\,i\,c\,i\,e\,n\,t)$ зашифрованное сообщение $C = (g\,h\,k\,g\,i\,g\,g\,j\,o\,c\,l)$.

При шифровке сообщение следует разбить на слова длиной p, и шифровать каждое слово отдельно. Слово длины p, очевидно, шифруется одинаково независимо от его положения в сообщении. Детальное изучение криптоустойчивости данного и близких к нему алгоритмов предполагается в дальнейшем.

Работа выполнена при финансовой поддержке гранта Президента РФ (проект НШ-4383.2010.1) и РФФИ (проект 10-01-00097-а).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Агаев Г. Н., Виленкин Н. Я., Джафарли Г. М., Рубинштейн А. И.* Мультипликативные системы функций и гармонический анализ на нуль-мерных группах. Баку : Элм, 1981.

2. *Лукомский С. Ф.* Кратномасштабный анализ на нуль-мерных абелевых группах и всплесковые базисы // Мат. сб. 2010. Т. 201, № 5. С. 41–46.

3. *Саломаа А.* Криптография с открытым ключом. М. : Мир, 1995.

УДК 517.984

Т. В. Мазур

АЛГОРИТМ РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ ШТУРМА — ЛИУВИЛЛЯ НА ЗВЕЗДООБРАЗНОМ ГРАФЕ

В статье предлагается алгоритм решения обратной задачи Штурма — Лиувилля на звездообразном графе, использующий ряд соотношений метода спектральных отображений и требующий относительно небольшого количества операций.

Пусть T – граф-звезда с множеством вершин $\{v_j\}_{j=0}^p$ и множеством рёбер $\{e_j\}_{j=1}^p$, $e_j = [v_0, v_j]$. Предположим, что длина каждого ребра равна 1. Каждое ребро рассматривается как отрезок $[0,1]$ и параметризуется параметром $x \in [0,1]$. Для нас удобно выбрать следующую ориентацию на каждом ребре: $x = 1$ соответствует вершине v_0.

Функция Y на T может быть представлена как вектор $Y(x) = [y_j(x)]_{j=1}^p$, $x \in [0,1]$. Пусть $q = [q_j(x)]_{j=1}^p$ – вещественнозначная функция на T такая, что $q_j(x) = \sigma_j'(x)$, $\sigma_j \in L_2[0,1]$. Назовём функцию $\sigma = [\sigma_j(x)]_{j=1}^p$ *потенциалом*. Дифференциальный оператор Штурма — Лиувилля на ребре e_j определяется следующим выражением [1]:

$$l_j y_j = -(y_j^{[1]})' - \sigma_j(x) y_j^{[1]} - \sigma_j^2(x) y_j,$$

где $y_j^{[1]} := y_j' - \sigma_j y_j$ – квазипроизводная, и

$$dom(l_j) = y_j | y_j \in W_2^1[0,1], y_j^{[1]} \in W_1^1[0,1], l_j y_j \in L_2[0,1].$$

Рассмотрим уравнение Штурма — Лиувилля на T:

$$l_j y_j = \lambda y_j, \quad x \in [0,1], \quad j = \overline{1,p}, \tag{1}$$

где $y_j \in dom(l_j)$, и функции y_j удовлетворяют следующим условиям склейки во внутренней вершине v_0:

$$y_j(1) = y_k(1), \quad j,k = \overline{1,p}, \tag{2}$$

$$\sum_{j=1}^{p} y_j^{[1]}(1) = 0. \tag{3}$$

Обозначим $U_j(Y) := y_j^{[1]}(0)$, $j = \overline{1,p}$, и рассмотрим краевую задачу B_0 для уравнения (1) с условиями склейки (2), (3) и с краевыми условиями

$$U_j(Y) = 0, \quad j = \overline{1,p}.$$

Мы также будем рассматривать краевые задачи B_k, $k = \overline{1,p}$, для уравнения (1) с условиями склейки (2), (3) и с краевыми условиями

$$y_k(0) = 0, \quad U_j(Y) = 0, \quad j = \overline{1,p} \backslash k.$$

Пусть $\Phi_k(x,\lambda) = [\Phi_{kj}(x,\lambda)]_{j=1}^p$, $k = \overline{1,p}$ – решения уравнения (1), удовлетворяющие (2), (3) и краевым условиям

$$U_j(\Phi_k) = \delta_{jk}, \tag{4}$$

где δ_{jk} – символ Кронекера. Обозначим $M_k(\lambda) := \Phi_{kk}(0,\lambda)$, $M(\lambda) = [M_k(\lambda)]_{k=1}^{p-1}$. Функция $M_k(\lambda)$ называется *функцией Вейля* для уравнения (1) относительно вершины v_k. $M(\lambda)$ называется *вектором Вейля*. Рассмотрим следующую обратную задачу.

Задача. По заданному вектору Вейля M определить потенциал σ.

Отметим, что понятие вектора Вейля является обобщением понятия функции Вейля (m-функции) для классического оператора Штурма — Лиувилля на интервале [2]. Как и в классическом случае, можно показать, что функции $M_k(\lambda)$ являются мероморфными по λ:

$$M_k(\lambda) = \frac{\Delta_k(\lambda)}{\Delta_0(\lambda)},$$

где $\Delta_k(\lambda)$ являются характеристическими функциями краевых задач B_k. Нули $\Lambda_k := \{\lambda_{kn}\}_{n\geq 0}$ целой функции $\Delta_k(\lambda)$ вещественны и совпадают с собственными значениями B_k.

Наряду с T рассмотрим дерево $\tilde{T}$ того же вида, но с другим потенциалом $\tilde{\sigma}$. Всюду далее, если символ α обозначает объект, относящийся к T, то $\tilde{\alpha}$ будет обозначать аналогичный объект, относящийся к $\tilde{T}$, и $\hat{\alpha} := \alpha - \tilde{\alpha}$.

Согласно [1] задание вектора Вейля M однозначно определяет потенциал σ на T. Решение обратной задачи может быть получено по формуле

$$\sigma_k(x) = -m_k(x) - \frac{1}{\pi i}\int_\Gamma \hat{\varphi}_k(x,\lambda)\tilde{\varphi}_k(x,\lambda)\hat{M}_k(\lambda)d\lambda, \tag{5}$$

где

$$m_k(x) = \frac{1}{\pi i}\lim_{N\to\infty}\int_{\gamma_N} \rho\hat{M}_k(\rho^2)\cos 2\rho x d\rho, \tag{6}$$

а $\varphi_k(x,\lambda)$ – решения уравнения (1) на ребре e_k при начальных условиях

$$\varphi_k(0,\lambda) = 1, \quad \varphi_k^{[1]}(0,\lambda) = 0. \tag{7}$$

γ – контур в ρ-плоскости, $\gamma = \gamma(\tau) := (-\infty + i\tau, +\infty + i\tau)$, где $\tau > 0$ такое, что $inf\{\Lambda_k \cup \tilde{\Lambda_k}\} > -\tau^2$. Γ – контур в λ-плоскости, являющийся отображением γ при $\lambda = \rho^2$.

Пусть задан вектор Вейля M, также пусть выбран и зафиксирован модельный оператор с потенциалом $\tilde{\sigma}$. Введём отображение S: по заданному σ построим для каждого λ решения $\varphi_k(x,\lambda)$ задачи Коши (1), (7). Подставляя найденные таким образом $\varphi_k(x,\lambda)$ в правые части соотношений (5), (6), получим новый потенциал $\bar{\sigma}$. Определим S как отображение,

ставящее потенциалу σ в соответствие полученный указанным способом потенциал $\bar{\sigma}$. Из предыдущего ясно, что потенциал σ^0, являющийся решением обратной задачи для данного M, является неподвижной точкой отображения S. Наряду с отображением S рассмотрим отображение S_N, определяемое так же, как и S, но с заменой в правой части (6) бесконечного контура на $\gamma_N = \gamma_N(\tau) := (-N + i\tau, N + i\tau)$. Предлагаемый численный метод решения обратной задачи состоит в том, что в качестве приближённого решения принимается неподвижная точка отображения S_N, которая ищется с помощью метода последовательных приближений [3]. При этом число N должно быть выбрано до начала итераций, исходя из предварительного анализа данных, а также из имеющейся априори информации о решении.

Алгоритм. Дан вектор Вейля $M(\lambda)$.

1. Выбираем модельную задачу $\tilde{B}$. Например, $\tilde{\sigma}_k(x) = 0$. Выбираем N.

2. Выбираем начальное приближение: $\sigma_k^{(0)} := \tilde{\sigma}_k(x)$.

3. Для каждого $r = 0, 1, 2, ...$ выполняем следующие шаги:

(i) для $\sigma_k = \sigma_k^{(r-1)}$ находим $\varphi(x, \lambda)$ как решение задачи Коши (1), (7).

(ii) находим следующее приближение из соотношений

$$\sigma_k^{(r)}(x) = -m_k(x) - \frac{1}{\pi i} \int_\Gamma (\varphi_k(x, \lambda) - \tilde{\varphi}_k(x, \lambda)) \tilde{\varphi}_k(x, \lambda) \hat{M}_k(\lambda) d\lambda,$$

$$m_k(x) = \frac{1}{\pi i} \int_{\gamma_N} \rho \hat{M}_k(\rho^2) \cos 2\rho x d\rho.$$

Для прекращения итераций можно использовать любой из общепринятых критериев.

Проведённые численные эксперименты показали, что метод сходится достаточно быстро (для широкого класса задач при выборе $20 \le N \le 50$ для достижения хорошего качества восстановления оказалось достаточно 10 – 20 итераций).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Freiling G., Ignatiev M., Yurko V.* An inverse spectral problem for Sturm — Liouville operators with singular potentials on star-type graphs // Proceedings of Symposia in Pure Mathematics. 2008. Vol. 77. P. 397 – 408.

2. *Юрко В. А.* Введение в теорию обратных спектральных задач. М. : Физматлит, 2007. 384 с.

3. *Ignatiev M., Yurko V.* Numerical Methods for Solving Inverse Sturm — Liouville Problems // Result. Math. 2008. Vol. 52. P. 63 – 74.