$$A_n = AB_{n-1},\ \frac{trA_n}{n} = q_n,\ B_n = A_n - q_n E. \qquad (1)$$

Moreover, the following statements are true:

1) $q_i = p_i,\ i = \overline{1,n}$ – i.e. these are the coefficients $P_A(\lambda)$,

2) $B_n = 0$,

3) if A – nondegenerate, then $A^{-1} = \frac{B_{n-1}}{q_n}$.

To find the eigenvectors of the matrix *A*, intermediate results of computations are used when constructing the eigenpolynomial of the matrix *A*.

Consider the matrix $Q(\lambda) = \lambda^{n-1}E + \lambda^{n-2}B_1 + \ldots + \lambda B_{n-2} + B_{n-1}$. Let us prove that if all the eigenvalues $\lambda_1,\ldots,\lambda_n$ of the original matrix *A* are different, then the matrices $Q(\lambda_i)\ (i = \overline{1,n})$ – nonzero and any nonzero matrix column $Q(\lambda_i)$ can be taken as an eigenvector of the matrix *A* corresponding to the eigenvalue λ_i.

Indeed

$$(\lambda_i E - A)Q(\lambda_i) = (\lambda_i E - A)(\lambda_i^{n-1}E + \lambda_i^{n-2}B_1 + \ldots +$$

$$+ \lambda_i B_{n-2} + B_{n-1}) = \lambda_i^n E + \lambda_i^{n-1}(B_1 - A) + \ldots +$$

$$+ \lambda_i (B_{n-1} - AB_{n-2}) - AB_{n-1} = (\lambda_i^n - p_1\lambda_i^{n-1} - \ldots - p_n)E = 0,$$

since it follows from (1) that $B_k - AB_{k-1} = -p_k E\ (k = \overline{1,n}),\ \lambda_i$ – there is root of a proper polynomial. From here $(\lambda_i E - A)Q(\lambda_i) = 0,$ means, $(\lambda_i E - A)\bar{x} = \bar{0}$ or $A\bar{x} = \lambda_i \bar{x},$ where $\bar{x}$ – native matrix column $Q(\lambda_i).$

When finding the eigenvectors of the matrix *A* in this way, it is not necessary to construct the entire matrix $Q(\lambda_i),$ but enough for everyone $\lambda_i (i = \overline{1,n})$ confine oneself to calculating only one of its columns.

In the case of multiple eigenvalues, the problem of finding the eigenvectors becomes more complicated: along with the matrix $Q(\lambda)$ we will have to involve the matrices obtained by differentiating it with respect to λ.

УДК 517.95

О ПРИМЕНЕНИИ МЕТОДА ФАКТОРИЗАЦИИ К РЕШЕНИЮ ЗАДАЧИ КОШИ ДЛЯ ГИПЕРБОЛИЧЕСКОГО УРАВНЕНИЯ ВТОРОГО ПОРЯДКА НА ПЛОСКОСТИ

М. Г. Ногач

Брестский государственный университет имени А. С. Пушкина, г. Брест

Научный руководитель: А. И. Басик, кандидат физ.-мат. наук, доцент

Одной из основных задач изучаемых студентами в курсах «Уравнения математической физики» и «Уравнения с частными производными», является задача Коши для уравнения второго порядка гиперболического типа на плоскости. Традиционно, при построении решения задачи Коши, как на лекционных,

так и на практических занятиях используется метод характеристик, известный также как метод Даламбера или метод бегущих волн. В известном учебнике А. Н. Тихонова и А. А. Самарского [1, с. 52] говорится, что «…, изложенный метод доказывает как единственность, так и существование решения поставленной задачи», что подтверждает универсальность метода характеристик. В настоящей статье мы приведем пример использования метода факторизации (разложения на множители) дифференциального оператора при построении решения задачи Коши. Этот метод с успехом применяется в теории обыкновенных дифференциальных уравнений [2, с. 56] и состоит в последовательном интегрировании задач Коши для линейных уравнений первого порядка. В книге [3, с. 16] методом факторизации получена формула общего решения однородного уравнения малых поперечных колебаний струны. Покажем на примере решения номера 12.10 из задачника [4], что этот метод применим и при построении решения задачи Коши для гиперболического уравнения на плоскости.

Задача. *Найти функцию* $u=u(x;y)$, *удовлетворяющую в* $\mathbf{R}^2$ *уравнению*

$$u_{xx} - u_{yy} - 2u_x - 2u_y = 4 \quad (1)$$

и начальным условиям

$$u\big|_{x=0} = -y, \quad u_x\big|_{x=0} = y - 1 \quad (-\infty < y < +\infty). \quad (2)$$

Решение. Разложение на множители левой части уравнения (1) имеет вид

$$u_{xx} - u_{yy} - 2u_x - 2u_y = \left(\frac{\partial}{\partial x} + \frac{\partial}{\partial y}\right)\left(\frac{\partial}{\partial x} - \frac{\partial}{\partial y} - 2\right)u.$$

Обозначим

$$z(x;y) = u_x - u_y - 2u.$$

Тогда функция $z(x;y)$ удовлетворяет уравнению

$$z_x + z_y = 4 \quad (3)$$

и начальному условию

$$z\big|_{x=0} = u_x\big|_{x=0} - u_y\big|_{x=0} - 2u\big|_{x=0} = y - 1 - (-1) - 2(-y) = 3y. \quad (4)$$

Построим решение задачи Коши (3), (4), методом описанным в [2, с. 275]. Для этого параметризуем начальные условия (4): $x=0$, $y=\tau$, $z=3\tau$, $\tau \in \mathbf{R}$. Характеристическая система для уравнения (3)

$$\dot{x}(t) = 1, \quad \dot{y}(t) = 1, \quad \dot{z}(t) = 4,$$

при начальных условиях

$$x\big|_{t=0} = 0, \quad y\big|_{t=0} = \tau, \quad z\big|_{t=0} = 3\tau,$$

имеет решение

$$x = t, \quad y = t + \tau, \quad z = 4t + 3\tau. \quad (5)$$

Исключая из формул (5) параметры t и τ, найдем решение (3), (4):

$$z(x;y) = x + 3y.$$

Возвращаясь к замене, для отыскания функции $u(x;y)$ получим задачу Коши

$$u_x - u_y = 2u + x + 3y, \quad u\big|_{x=0} = -y. \quad (6)$$

Рассуждая также как и при решении (3), (4), составим характеристическую систему для уравнения в (6)

$$\dot{x}(t) = 1, \quad \dot{y}(t) = -1, \quad \dot{u}(t) = 2u + x + 3y$$

при начальных условиях

$x(0)=0,\ \ y(0)=\tau,\ \ u(0)=-\tau\ \ (\tau\in\mathbf{R}).$

Параметрическое решение последней системы имеет вид

$$x=t,\ \ y=-t+\tau,\ \ u=\frac{\tau-1}{2}e^{2t}+t+\frac{1-3\tau}{2}.$$

Отсюда найдем явное решение исходной задачи Коши

$$u(x;y)=\frac{x+y-1}{2}e^{2x}+\frac{1-x-3y}{2}.$$

Ответ: $u(x;y)=\dfrac{x+y-1}{2}e^{2x}+\dfrac{1-x-3y}{2}.$

Список литературы

1. Тихонов, А. Н. Уравнения математической физики : учеб. пособие / А. Н. Тихонов, А. А. Самарский. – М. : Наука, 1977. – 736 с.
2. Романко, В. К. Курс дифференциальных уравнений и вариационного исчисления / В. К. Романко. – М.: Лаборатория Базовых Знаний, 2000. – 344 с.
3. Берс, Л. Уравнения с частными производными / Л. Берс, Ф. Джон, М. Шехтер. – М. : Мир, 1966. – 352 с.
4. Сборник задач по уравнениям математической физики / В. С. Владимиро [и др.]. – М. : ФИЗМАТЛИТ, 2016. – 520 с.

УДК 004.056.55

ПРИМЕР ПОСТРОЕНИЯ АЛГОРИТМА ШИФРОВАНИЯ

М.А. Протько

Белорусский государственный университет информатики и радиоэлектроники, г. Минск.

Научный руководитель: О.Ф. Борисенко, канд. физ.-мат. наук, доцент

Введение. Что составляет любой базовый криптографический алгоритм? По сути, это два соответствия: базовый/шифрованный текст. Связь между первым и вторым происходит по некой функции F с приблизительно следующими свойствами:

$F(B)=A$ – легко рассчитываемая функция.

$B=F^{-1}(A)$ – не вычисляемая функция доступными средствами.

То есть задача построения алгоритма шифрования будет соответствовать следующей формулировке:

Пусть K – пространство ключей, e и d – ключи шифрования и расшифрования соответственно. E_e – односторонняя функция шифрования для произвольного ключа e ∈ K, такая, что $E_e(t)=c$, c ∈ C, C - пространство шифротекстов, t ∈ T, T – пространство сообщений. D_d – функция расшифрования, такая, что $D_d(c) = t$. Каждая пара (E,D) имеет свойство: зная E_e невозможно найти $E_e(t)=c$.

Учитывая необходимость в вычислительной сложности таковых функций, простой перебор всех возможных значений и применение принципа индукции могут не дать доказательства их верности. Для более качественной оценки по-