числительно трудных задач // Вопр. защиты информации. 2008. № 1. С. 22–26.

3. Дернова Е. С., Молдовян Н. А. Протоколы коллективной цифровой подписи, основанные на сложности решения двух трудных задач // Безопасность информационных технологий. 2008. № 2. С. 79–85.

4. Blind Signature Protocol Based on Difficulty of Simultaneous Solving Two Difficult Problems / N. H. Minh, D. V. Binh, N. T. Giang, N. A. Moldovyan // Appl. Mathematical Sciences. 2012. Vol. 6, № 139. P. 6903–6910.

5. Do B. V., Nguyen M. H., Moldovyan N. A. Digital Signature Schemes from Two Hard Problems // Lecture Notes in Electrical Engineering. 2013. Vol. 240. LNEE. P. 817–825.

6. Протокол групповой цифровой подписи на основе маскирования открытых ключей / А. А. Молдовян, Н. А. Молдовян, Д. М. Латышев, Д. А. Головачев // Вопр. защиты информации. 2011. № 3. С. 2–6.

7. Gordon J. Strong primes are easy to find // Advances in cryptology – EUROCRYPT'84. Springer-Verlag LNCS. 1985. Vol. 209. P. 216–223.

8. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. 323 с.

9. Moldovyan A. A., Moldovyan N. A. Group signature protocol based on masking public keys // Quasigroups and related systems. 2014. Vol. 22. P. 133–140.

10. Menezes A. J., Oorshort P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996. 780 p.

V. E. Sinev
Saint Petersburg Electrotechnical University «LETI»

INCREASING THE LEVEL OF SECURITY OF THE PROTOCOL GROUP DIGITAL SIGNATURE BASED ON THE MASKING MECHANISM OF PUBLIC KEYS

First we consider the problem of raising the level of security protocols, group signature based on the masking mechanism of public keys of signers and a suggestion for solution of practical interest. Developed a Protocol based on computational difficulty of simultaneously solving the problem of factorization and discrete logarithm problem for a Prime modulus.

Cryptographic algorithms, cryptographic protocols, group digital signature, masking the public keys

УДК 517.443

А. С. Колпаков, Ан. Ю. Филатов, Ар. Ю. Филатов
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

О скорости сходимости рядов Фурье специального вида

Рассматривается аппроксимация суммируемой функции частичными рядами Фурье только по косинусам или только по синусам. Рассматривается теорема, описывающая скорость приближения функции такими частичными рядами в зависимости от ограничений на исходную функцию. Полученные результаты позволяют выделить разницу между разложениями в ряд Фурье только по косинусам или только по синусам.

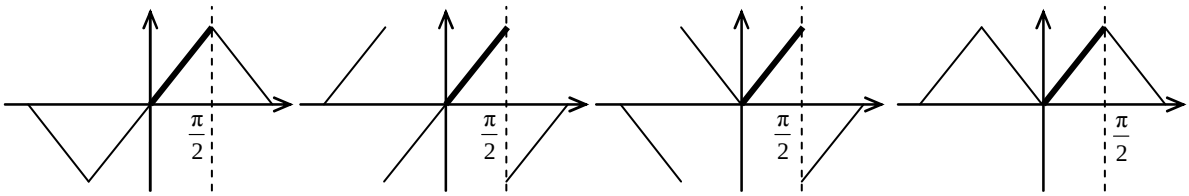
Ряд Фурье, синусы, косинусы, ядро Дирихле, свертка, частичная сумма, скорость сходимости

Хорошо известно, что в задачах операционного исчисления, широко применяемого при решении дифференциальных уравнений, самым трудным является шаг восстановления оригинала по найденному изображению. В задачах, решаемых на практике, на этом этапе могут появиться трудности, если к изображению невозможно применить таблицы. В связи с этим развиваются различные методы обращения.

Так, в [1, с. 25] рассматривается метод обращения преобразования Лапласа при помощи рядов Фурье. Перейдя от поиска оригинала, где $x \in (0, \infty)$, к функции

$$\varphi(t) = f\left(-\frac{1}{\sigma}\ln\cos t\right),$$

где $t \in \left(0, \frac{\pi}{2}\right)$ – аргумент функции; σ – некоторый параметр $y(x)$, авторы предлагают искать новую функцию в виде ряда Фурье по синусам нечетных дуг, т. е. в виде



а *б* *в* *г*

$$\varphi(t)=\sum_{k=0}^{\infty} c_k \sin\left((2k+1)t\right),$$

где c_k – коэффициенты ряда Фурье.

При этом никак не комментируется оптимальность выбора именно этого разложения, а не, например, разложения по косинусам нечетных дуг. Ведь ясно, что функция $\varphi(t)$, суммируемая на $(0,\pi/2)$, допускает разложения в ряды Фурье как только по синусам нечетных дуг, так и по синусам четных дуг, а также по косинусам четных и нечетных дуг. Для этого стоит правильным образом продолжить ее за пределы $(0,\pi/2)$. Так на рисунке, *а* показано продолжение для разложения в ряд Фурье только по синусам нечетных дуг; *б* – синусам четных дуг; *в* – косинусам нечетных дуг; *г* – косинусам четных дуг.

В поисках ответа был поставлен более общий вопрос (не имеющий отношения к преобразованию Лапласа): различна ли скорость сходимости хотя бы у хорошо известных разложений в ряд Фурье функции *f*, суммируемой на $(0,\pi)$, только по косинусам и только по синусам в зависимости от ограничений на эту функцию.

Классической является формула, связывающая частичную сумму ряда Фурье для функции, суммируемой на интервале $(-\pi,\pi)$, с ядром Дирихле *n*-го порядка [2, с. 501]:

$$D_n(t)=\frac{1}{2}+\sum_{k=1}^{n}\cos(kt)=\frac{\sin\left((n+1/2)t\right)}{2\sin(t/2)}, \quad (1)$$

при этом

$$\frac{2}{\pi}\int_0^{\pi} D_n(t)\,dt=1, \quad (2)$$

и с самой функцией:

$$S_n(f,x)=\frac{1}{\pi}\int_{-\pi}^{\pi} f(x+t)D_n(t)\,dt.$$

Попробовать дать ответ на поставленный ранее вопрос можно, выведя аналогичные представления частичной суммы ряда Фурье только по косинусам и только по синусам для функции, суммируемой на интервале $(0,\pi)$. Пусть сначала функция $f(x)$ разложена в ряд Фурье только по косинусам. Тогда ее частичная сумма имеет следующий вид:

$$S_n^{\cos}(x)=\frac{a_0}{2}+\sum_{k=1}^{n} a_k\cos(kx),$$

где $a_k=\frac{2}{\pi}\int_0^{\pi} f(t)\cos kt\,dt$.

Подставив выражения для коэффициентов в формулу частичной суммы и поменяв местами интеграл и сумму, получим:

$$S_n^{\cos}(x)=\frac{1}{\pi}\int_0^{\pi} f(t)\left(1+2\sum_{k=1}^{n}\cos(kx)\cos(kt)\right)dt.$$

Далее применяем формулу произведения косинусов:

$$S_n^{\cos}(x)=$$
$$=\frac{1}{\pi}\left(\int_0^{\pi} f(t)D_n(x-t)\,dt+\int_0^{\pi} f(t)D_n(x+t)\,dt\right).$$

Заменив $x-t$ и $x+t$ в соответствующих интегралах новыми переменными, перейдем к такой замене, где ядра Дирихле не зависят от *x*:

$$S_n^{\cos}(x)=$$
$$=\frac{1}{\pi}\left(\int_{-x}^{\pi-x} f(x+t)D_n(t)\,dt+\int_{x}^{\pi+x} f(t-x)D_n(t)\,dt\right).$$

Теперь каждый интеграл разобьем на два так, чтобы отделить части, выходящие за интервал $(0,\pi)$:

$$S_n^{\cos}(x)=\frac{1}{\pi}\left(\int\limits_{-x}^{0} f(x+t)D_n(t)\,dt+\right.$$
$$+\int\limits_{0}^{\pi-x} f(x+t)D_n(t)\,dt+$$
$$+\int\limits_{x}^{\pi} f(t-x)D_n(t)\,dt+$$
$$\left.+\int\limits_{\pi}^{\pi+x} f(t-x)D_n(t)\,dt\right).$$

Приняв $-t$ в первом интеграле и $2\pi-t$ в четвертом интеграле за новые переменные, в силу четности и 2π-периодичности ядра Дирихле получим:

$$S_n^{\cos}(x)=\frac{1}{\pi}\left(\int\limits_{0}^{x} f(x-t)D_n(t)\,dt+\right.$$
$$+\int\limits_{0}^{\pi-x} f(x+t)D_n(t)\,dt+$$
$$+\int\limits_{x}^{\pi} f(t-x)D_n(t)\,dt+$$
$$\left.+\int\limits_{\pi-x}^{\pi} f(2\pi-t-x)D_n(t)\,dt\right).$$

Ясно, что аргументы в первом и третьем интегралах – это различные представления выражения $|x-t|$ в зависимости от того, $t\in(0,x)$ или же $t\in(x,\pi)$. Аналогично, выражение $|\pi-(\pi-(x+t))|$ равно аргументам второго и четвертого интегралов в зависимости от принадлежности t к соответствующему из промежутков $(0,\pi-x)$ и $(\pi-x,\pi)$. Таким образом, после группировки переходим к формуле

$$S_n^{\cos}(x)=\frac{1}{\pi}\times$$
$$\times\int\limits_{0}^{\pi}\Big(f\big(\big|\pi-\big|\pi-(x+t)\big|\big|\big)+f\big(|x-t|\big)\Big)D_n(t)\,dt. \quad (3)$$

Проделаем аналогичные действия, чтобы получить представление частичной суммы ряда Фурье только по синусам для функции, суммируемой на $(0,\pi)$, через ядро Дирихле и саму функцию:

$$S_n^{\sin}(x)=\sum_{k=1}^{n} b_k\sin(kx),$$

где $b_k=\frac{2}{\pi}\int\limits_{0}^{\pi} f(t)\sin kt\,dt$.

Подставив выражение коэффициентов в формулу частичной суммы и поменяв местами интеграл и сумму, получим:

$$S_n^{\sin}(x)=\frac{2}{\pi}\int\limits_{0}^{\pi} f(t)\left(\sum_{k=1}^{n}\sin(kx)\sin(kt)\right)dt.$$

Далее применяем формулу произведения синусов:

$$S_n^{\sin}(x)=$$
$$=\frac{1}{\pi}\left(\int\limits_{0}^{\pi} f(t)D_n(x-t)\,dt-\int\limits_{0}^{\pi} f(t)D_n(x+t)\,dt\right).$$

Сделав соответствующие замены и разбив каждый из интегралов на два, получим следующую сумму:

$$S_n^{\sin}(x)=\frac{1}{\pi}\left(\int\limits_{0}^{x} f(x-t)D_n(t)\,dt+\right.$$
$$+\int\limits_{0}^{\pi-x} f(x+t)D_n(t)\,dt-$$
$$-\int\limits_{x}^{\pi} f(t-x)D_n(t)\,dt-$$
$$\left.-\int\limits_{\pi-x}^{\pi} f(2\pi-x-t)D_n(t)\,dt\right).$$

Заметим, что $f(-t+x)$ и $-f(t-x)$ в первом и третьем интегралах – это различные представления выражения $\operatorname{sign}(x-t)\,f(|x-t|)$ в зависимости от промежутка изменения переменной t. Аналогично во втором и в четвертом интегралах $f(t+x)$ и $f(2\pi-t-x)$ – это различные представления выражения $\operatorname{sign}\big(\pi-(x+t)\big)\,f\Big(\big|\pi-\big|\pi-(x+t)\big|\big|\Big)$. Тогда

$$S_n^{\sin}(x)=\frac{1}{\pi}\int\limits_{0}^{\pi}\Big(\operatorname{sign}\big(\pi-(x+t)\big)\,f\Big(\big|\pi-\big|\pi-(x+t)\big|\big|\Big)+$$
$$+\operatorname{sign}(x-t)\,f\big(|x-t|\big)\Big)D_n(t)\,dt. \quad (4)$$

Формулы (3) и (4) выражают частичные суммы рядов Фурье для разложения функции f, суммируемой на $(0,\pi)$, только по косинусам и только по синусам.

Теперь перейдем к изучению скорости сходимости частичной суммы ряда Фурье для функции f к самой функции в зависимости от дополнительных ограничений на f. Начнем с разложения только по косинусам.

Теорема. Если для дважды дифференцируемой функции, у которой вторая производная суммируема, выполняется $f'(0) = f'(\pi) = 0$, то

$$\left|S_n^{\cos}(x) - f(x)\right| = o\left(n^{-2}\right),$$

где $o(f)$ – функция с большим порядком малости.

Доказательство. Рассмотрим модуль разности частичной суммы и функции $f(x)$, которая была разложена в ряд Фурье только по косинусам:

$$\left|S_n^{\cos}(x) - f(x)\right| = \frac{1}{\pi}\left|\int_0^{\pi}\left(f\left(\left|\pi - \left|\pi - (x+t)\right|\right|\right) + \right.\right.$$

$$\left.\left. + f(|x-t|)\right) D_n(t)\,dt - f(x)\right|. \quad (5)$$

В силу (2) второе слагаемое под модулем можно домножить на интеграл от ядра Дирихле. Представив его после этого в виде отношения синусов (1), перепишем формулу (5) в следующем виде:

$$\left|S_n^{\cos}(x) - f(x)\right| = \frac{1}{\pi}\times$$

$$\times\left|\int_0^{\pi}\frac{f\left(\left|\pi - \left|\pi - (x+t)\right|\right|\right) + f(|x-t|) - 2f(x)}{2\sin t/2}\times\right.$$

$$\left.\times\sin\left(\left(n+\frac{1}{2}\right)t\right)dt\right|.$$

Введя обозначение

$$h(t,x) = \frac{f\left(\left|\pi - \left|\pi - (x+t)\right|\right|\right) + f(|x-t|) - 2f(x)}{2\sin t/2}, \quad (6)$$

приведем ее к виду

$$\left|S_n^{\cos}(x) - f(x)\right| = \frac{1}{\pi}\left|\int_0^{\pi} h(t,x)\sin\left(\left(n+\frac{1}{2}\right)t\right)dt\right|. \quad (7)$$

Если $h(t,x)$ – суммируема, то по лемме Римана–Лебега [2, с. 463] значение интеграла стремится к нулю при $n \to \infty$. Попробуем усилить этот результат. Если $h'(t,x)$ – суммируема, то интеграл можно взять по частям:

$$\left|S_n^{\cos}(x) - f(x)\right| = \frac{1}{\pi\left(n+\frac{1}{2}\right)}\times$$

$$\times\left|h(0,x) + \int_0^{\pi} h'(t,x)\cos\left(\left(n+\frac{1}{2}\right)t\right)dt\right|.$$

Таким образом, если показать, что $h(0,x) = 0$, то интеграл из (7) будет стремиться к нулю по лемме Римана–Лебега, и модуль разности частичной суммы и функции будет стремиться к нулю со скоростью $o(n^{-1})$:

$$h(0,x) =$$

$$= \lim_{t\to 0}\frac{f\left(\left|\pi - \left|\pi - (x+t)\right|\right|\right) + f(|x-t|) - 2f(x)}{2\sin t/2}. \quad (8)$$

Здесь нужно различать 3 ситуации:

1) $x = 0$, тогда

$$h(0,0) = \lim_{t\to 0}\frac{f\left(\left|\pi - \left|\pi - t\right|\right|\right) + f(|t|) - 2f(0)}{2\sin t/2}.$$

После очевидного раскрытия модулей перепишем это выражение в следующем виде:

$$h(0,0) = \lim_{t\to 0}\frac{f(t) + f(t) - 2f(0)}{2\sin t/2} = f'(0);$$

2) $x = \pi$, тогда

$$h(0,\pi) = \lim_{t\to 0}\frac{f\left(\left|\pi - \left|\pi - (\pi+t)\right|\right|\right) + f(|\pi - t|) - 2f(\pi)}{2\sin\ t/2}.$$

После очевидного раскрытия модулей перепишем это выражение в следующем виде:

$$h(0,\pi) = \lim_{t\to 0}\frac{f(\pi - t) + f(\pi - t) - 2f(\pi)}{2\sin t/2} = f'(\pi);$$

3) $x \in (0,\pi)$, тогда

$$h(0,x) = \lim_{t\to 0}\frac{f\left(\left|\pi - \left|\pi - (x+t)\right|\right|\right) + f(|x-t|) - 2f(x)}{2\sin\ t/2}.$$

В силу того, что x фиксирован, а $t \to 0$, ясно, что $x - t > 0, x + t < \pi$, тогда (8) можно привести к виду

$$h(0,x) = \lim_{t\to 0}\frac{f(x+t) + f(x-t) - 2f(x)}{2\sin t/2}.$$

Здесь в числителе первое и второе слагаемые можно разложить в ряд Тейлора в окрестности точки x. Для этого необходимо, чтобы $f(x)$ была хотя бы один раз дифференцируема. Тогда

$$h(0,x) = \lim_{t\to 0} f(x) + f'(x)t + o(t) + f(x) -$$

$$- f'(x)t + o(t) - 2f(x)/2\sin t/2 = 0.$$

Таким образом, для выполнения условия

$$\left|S_n^{\cos}(x) - f(x)\right| = o\left(n^{-1}\right)$$

достаточно, чтобы

$$f'(0) = f'(\pi) = 0. \qquad (9)$$

Это условие выполнено. Тогда

$$\left|S_n^{\cos}(x) - f(x)\right| = \\ = \frac{1}{\pi\left(n+\frac{1}{2}\right)}\left|\int_0^{\pi} h'(t,x)\cos\left(\left(n+\frac{1}{2}\right)t\right)dt\right|.$$

Поскольку $f \in W_1^2$, то последний интеграл можно взять по частям:

$$\left|S_n^{\cos}(x) - f(x)\right| = \frac{1}{\pi\left(n+\frac{1}{2}\right)^2}\times \\ \times\left|(-1)^n h'(\pi,x) - \int_0^{\pi} h''(t,x)\sin\left(\left(n+\frac{1}{2}\right)t\right)dt\right|.$$

Решим аналогичную задачу – попытаться показать, при каких условиях $h_t'(\pi, x) = 0$.

Поскольку $h(t,x)$ вычисляется по (6), то прежде, чем брать производную, следует раскрыть модули. Для этого таким же образом следует разобрать 3 ситуации:

1) $x = 0$, тогда

$$h'(\pi,0) = \lim_{t\to\pi}\left(\frac{f\left(\left|\pi-\left|\pi-t\right|\right|\right) + f(|t|) - 2f(0)}{2\sin t/2}\right)_t'.$$

После очевидного раскрытия модулей перепишем это выражение в следующем виде:

$$h'(\pi,0) = \lim_{t\to\pi}\left(\frac{f(t) + f(t) - 2f(0)}{2\sin t/2}\right)_t' = f'(\pi);$$

2) $x = \pi$, тогда

$$h'(\pi,\pi) = \\ = \lim_{t\to\pi}\left(\frac{f\left(\left|\pi-\left|\pi-(\pi+t)\right|\right|\right) + f(|\pi-t|) - 2f(0)}{2\sin t/2}\right)_t'.$$

После очевидного раскрытия модулей перепишем это выражение в следующем виде:

$$h'(\pi,\pi) = \\ = \lim_{t\to\pi}\left(\frac{f(\pi-t) + f(\pi-t) - 2f(\pi)}{2\sin t/2}\right)' = -f'(0);$$

3) $0 < x < \pi$, тогда

$$h'(0,x) = \\ = \lim_{t\to 0}\left(\frac{f\left(\left|\pi-\left|\pi-(x+t)\right|\right|\right) + f(|x-t|) - 2f(x)}{2\sin t/2}\right)_t'.$$

Поскольку x фиксирован, а $t \to \pi$, ясно, что $x - t < 0$, $x + t > \pi$, поэтому

$$h'(\pi,x) = \lim_{t\to\pi}\left(\frac{f(2\pi-(t+x)) + f(t-x) - 2f(x)}{2\sin\ t/2}\right)' = \\ = \frac{-f'(\pi-x) + f'(\pi-x)}{2\sin\ t/2} = 0.$$

Таким образом, $h'(t,x)$ обращается в ноль при тех же условиях, что и (8), а именно при

$$f'(0) = f'(\pi) = 0.$$

Поскольку по условию теоремы это условие выполнено, то из (9) следует:

$$\left|S_n^{\cos}(x) - f(x)\right| = \frac{1}{\pi\left(n+\frac{1}{2}\right)^2}\times \\ \times\left|\int_0^{\pi} h''(t,x)\sin\left(\left(n+\frac{1}{2}\right)t\right)dt\right| = o\left(n^{-2}\right),$$

что завершает доказательство.

Заметим, что хотя могло показаться, будто подобные рассуждения можно проделывать бесконечно и ускорять сходимость, ограничивая функцию лишь на концах промежутка, уже на следующем шаге возникает сложность:

$$\left|S_n^{\cos}(x) - f(x)\right| = \frac{1}{\pi\left(n+\frac{1}{2}\right)^3}\times \\ \times\left|h''(0,x) - \int_0^{\pi} h'''(t,x)\sin\left(\left(n+\frac{1}{2}\right)t\right)dt\right|.$$

Рассматривая 3 возможные ситуации, получаем:

1) $h''(0,0) = f'''(0)$;

2) $h''(0,\pi) = f'''(\pi)$;

3) $h''(0,x) = \lim_{t\to 0}\frac{f''(x-t) + f''(x+t)}{2\sin t/2}$.

Таким образом, сходимость может быть быстрее, чем $o\left(n^{-2}\right)$, на краях промежутка, а также в точках, где вторая производная обращается в ноль.

Рассматривая частичную сумму ряда по синусам (4), можно получить результат:

$$f(0) = f(\pi) = 0 \Rightarrow \left| S_n^{\sin}(x) - f(x) \right| = o\left(n^{-2}\right).$$

В результате можно утверждать, что в зависимости от конкретных свойств, которым удовлетворяет функция f, суммируемая на $(0, \pi)$, следует предпочесть разложение только по косинусам или только по синусам. Этот положительный результат позволяет искать подобные различия для рядов Фурье по синусам нечетных или четных дуг, а также косинусам нечетных или четных дуг.

СПИСОК ЛИТЕРАТУРЫ

1. Крылов В. И., Скобля Н. С. Методы приближенного преобразования Фурье и обращения преобразования Лапласа. М.: Наука, 1974. 224 с.

2. Макаров Б. М., Подкорытов А. Н. Лекции по вещественному анализу. СПб.: БХВ-Петербург, 2011. 688 с.

A. S. Kolpakov, An. Yu. Filatov, Ar. Yu. Filatov
Saint Petersburg Electrotechnical University «LETI»

SPEED CONVERGENCE OF FOUTIER SERIES OF SPECIAL FORM

Approximation of integrable functions with partial Fourier series of cosine only or sine only. There is the theorem describing approximation speed of these series in depend of restrictions on the original function. The results obtained highlight the difference between the Fourier series only cosine or sine only.

Fourier series, sine, cosine, Dirichlet kernel, convolution, partial sum, approximation speed

УДК 613.6.02:613.97

А. О. Карелин
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Д. В. Павлова
Санкт-Петербургский государственный медицинский университет им. акад. И. П. Павлова

Сравнительная оценка подачи информации посредством традиционных и современных источников в обучении студентов

Приведены результаты исследований влияния на функциональное состояние организма студентов-медиков учебной работы с использованием различных носителей информации: традиционного (бумажного) и персонального компьютера. Установлено, что утомление при использовании персонального компьютера более выражено. Выявлено, что информация с традиционного бумажного носителя усваивается лучше.

Информация, компьютер, утомление, функциональное состояние, студенты

Компьютерная техника постоянно совершенствуется, создаются новые и видоизменяются уже существующие устройства, повышается возможность использования электронно-вычислительной техники. Уже невозможно представить ни одно учебное заведение без компьютерного обеспечения. Современные инфокоммуникационные технологии существенно расширяют возможности получения образования, позволяют оптимизировать средства доставки и разработки учебной ин-