Math-Net.Ru

Общероссийский математический портал

А. С. Рыбаков, Оценки количества чисел со специальным разложением на простые множители. II, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 3, 53–78

DOI: <https://doi.org/10.4213/mvk332>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.89.185.249

26 апреля 2023 г., 13:09:04

Оценки количества чисел со специальным разложением на простые множители. II

А. С. Рыбаков

Лаборатория ТВП, Москва

Получено 11.II.2020

Аннотация. Предлагаются методы вычисления значений некоторых обобщений известной функции Дикмана, позволяющие оценивать количество целых чисел в интервале большой длины, разлагающихся на простые множители со специфическими ограничениями. Методы основаны на найденных ранее автором интегральных формулах, обобщающих известные формулы из работ Р. Ламберта и В.Х. Эккелькампа.

Ключевые слова: функция Дикмана, разложение на множители, гладкие числа

Estimates of the number of integers with the special prime factorization. II

A. S. Rybakov

TPA Laboratory, Moscow

Abstract. We suggest computational methods for values of some generalizations of the well-known Dickman function. These generalizations may be used to estimate the number of integers in a long interval having prime factorization satisfying specific conditions. The methods are based on previously obtained by the author integral formulas generalizing results from papers by R.Lambert and W.H.Ekkelkamp.

Keywords: Dickman function, prime factorization, smooth numbers

1. Введение

В данной работе речь пойдет об эффективном вычислении значений некоторых обобщений хорошо известной функции Дикмана [8], а именно значений функций $(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2) \in (0; 1)^5 \rightarrow G_l(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2)$, $l = 1, 2, \dots$, равных по определению предельной при $x \rightarrow \infty$ вероятности того, что все простые делители p случайно выбранного целого числа отрезка $[1; x]$ меньше x^{β_0} за исключением точно l больших простых делителей q (с учетом кратностей), из которых первый (наименьший) большой простой делитель принадлежит промежутку $[x^{\alpha_1}; x^{\beta_1})$, а остальные большие простые делители принадлежат промежутку $[x^{\alpha_2}; x^{\beta_2})$ [5, 10].

Способы быстрого вычисления значений частных случаев функций G_l при некоторых значениях l и ограничениях на числа α_i и β_i исследовались в ряде работ [3, 4, 6, 7, 9]. В основе всех алгоритмов, предложенных в этих работах, использовались найденные авторами представления функций G_l в виде кратных интегралов кратности $\max(l - 1, 1)$. В частности, для случая $l = 1$ и $\alpha_1 = \beta_0$ быстрый алгоритм нахождения значений G_1 предложен в работе Э. Баха и Р. Перальты [6] в 1996 г., являющейся по существу исходной точкой развития всех дальнейших методов, касающихся функций более сложного вида. Сложность этого алгоритма составляет $O(n \ln n)$ арифметических операций с плавающей точкой и $O(1)$ операций нахождения значения логарифма, где $n = \lceil \frac{\beta_1}{\beta_0} \rceil + 1$.

Случай $l = 2$, $\alpha_1 = \alpha_2 = \beta_0 < \beta_1 = \beta_2$ разобран в диссертации Р. Ламберта [9], опубликованной также в 1996 г. В диссертации показано, что при том же значении n нахождение величины $G_2(\beta_0, \beta_0, \beta_1, \beta_0, \beta_1)$ проводится за $O(n \ln^3 n)$ операций сложения и умножения с плавающей точкой, $O(\ln n)$ операций деления и $O(n)$ операций нахождения значений логарифма и дилогарифма, где $\text{dilog}(x) = \int_1^x \frac{\ln t}{1-t} dt$. Это сделано с помощью найденного Р. Ламбертом представления функции G_2 в виде линейной комбинации интегралов кратности 1 (базовая интегральная формула для G_2 имеет кратность 2).

Алгоритм Р. Ламберта, а также найденные им интегральные формулы были обобщены в 2010 г. в работе В.Х. Эккелькампа [7] для $l = 2$, $\alpha_1 = \alpha_2 = \beta_0 < \beta_1 < \beta_2$, при этом приведенная выше оценка трудоемкости алгоритма осталась прежней.

Автор в [3] предложил более быстрый алгоритм оценки величин $G_2(\beta_0, \alpha_1, \beta_1, \alpha_1, \beta_1)$ и $G_3(\beta_0, \alpha_1, \beta_1, \alpha_1, \beta_1)$, требующий лишь $O(n \ln n)$ арифметических операций с плавающей точкой и $O(n)$ операций на-

хождения значения логарифма. При этом никаких других операций в методе не используется, в частности значения дилогарифма вычислять не нужно. В основе алгоритма лежат найденные автором $(l-1)$ -кратные интегральные формулы для G_l , $l = 2, 3$. Формулы для G_2 по существу совпадают с формулами, найденными Р. Ламбертом в более частном случае, однако записываются в более унифицированном и удобном для программирования виде.

Отметим, что случай $l = 3$ является существенно более трудным, чем случаи $l = 1, 2$, поскольку с ростом l растет и кратность интеграла в формуле, определяющей значение величины G_l . Базовая формула для G_3 представляет собой тройной интеграл. Понижение кратности интегрирования и построение алгоритма, аналогичного исходному алгоритму Э. Баха и Р. Перальты, является в данном случае намного более сложной задачей. Также отметим, что во всех упомянутых выше статьях параметры функций G_l удовлетворяли дополнительному ограничению $\beta_1 + (l-1)\beta_2 < 1$. Это ограничение обеспечивает выполнение условия $\prod_{i=1}^l q_i < x$, где $q_1 \in [x^{\alpha_1}; x^{\beta_1})$ и $q_i \in [x^{\alpha_2}; x^{\beta_2})$ при $i \geq 2$, позволяющего получить интегральные формулы, о которых шла речь.

В [4] автором были найдены $(l-1)$ -кратные интегральные формулы для функций G_l , $l = 2, 3$, при произвольных значениях аргументов, удовлетворяющих последнему ограничению. Эти формулы обобщают ранее известные формулы из упомянутых работ Р. Ламберта, В.Х. Эккелькампа, а также автора. В настоящей работе предлагаются методы вычисления найденных двукратных и трехкратных интегралов, являющиеся обобщениями методов работы [3] и имеющие аналогичную оценку трудоемкости $O(n \ln n)$ арифметических операций с плавающей точкой и $O(n)$ операций нахождения значения логарифма.

2. Формулы для G_2 и G_3

Пусть

$$G_l^{(1)}(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2) = \frac{1}{(l-1)!} \int_{\alpha_1}^{\beta_1} \int_{\alpha_2}^{\beta_2} \dots \int_{\alpha_2}^{\beta_2} \rho\left(\frac{1-\lambda_1-\dots-\lambda_l}{\beta_0}\right) \frac{d\lambda_l}{\lambda_l} \dots \frac{d\lambda_2}{\lambda_2} \frac{d\lambda_1}{\lambda_1}$$

и

$$G_l^{(2)}(\beta_0, \alpha_1, \beta_1, \beta_2) = \frac{1}{(l-1)!} \int_{\alpha_1}^{\beta_1} \int_{\alpha_1}^{\beta_2} \dots \int_{\alpha_1}^{\beta_2} \rho\left(\frac{1-\lambda_1-\dots-\lambda_l}{\beta_0}\right) \frac{d\lambda_l}{\lambda_l} \dots \frac{d\lambda_2}{\lambda_2} \frac{d\lambda_1}{\lambda_1},$$

где ρ – функция Дикмана. Согласно теореме 1 из [4] интересные нас значения $G_l(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2)$ вычисляются через введенные интеграль-

ные выражения следующим образом:

$$G_l(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2) = \begin{cases} G_l^{(1)}(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2), & \alpha_2 \geq \beta_1, \\ G_l^{(1)}(\beta_0, \alpha_1, \alpha_2, \alpha_2, \beta_2) + G_l^{(2)}(\beta_0, \alpha_2, \beta_1, \beta_2), & \alpha_2 < \beta_1. \end{cases}$$

Таким образом, вычисление значений функций G_l сводится к вычислению значений функций $G_l^{(1)}$ и $G_l^{(2)}$.

В [4] приведены теоремы 2 и 3, позволяющие уменьшить кратность интегрирования при вычислении интегралов $G_l^{(1)}$ и $G_l^{(2)}$. Однако этими теоремами можно пользоваться не при всех возможных значениях параметров. Существо дела хорошо показывает следующий числовой пример.

Пример 1. Попытаемся формально применить к интегралу

$$I = \int_{0.2}^{0.3} \int_{0.09+x}^{1.5x} \ln(1.8x - y) dy dx$$

лемму 1 из [4]. Имеем

$$I = \int_{0.29}^{0.39} \int_{0.2}^{y-0.09} \ln(1.8x - y) dx dy - \int_{0.3}^{0.39} \int_{0.2}^{0.3} \ln(1.8x - y) dx dy + \int_{0.3}^{0.45} \int_{2y/3}^{0.3} \ln(1.8x - y) dx dy.$$

Мы здесь поменяли местами внешний и внутренний интегралы в выражении для I , при этом исходный двойной интеграл представился в виде суммы трех слагаемых. Однако, как нетрудно заметить, подынтегральная функция не определена при значениях $x \approx 0.2$ и $y \approx 0.39$, так что выписанное равенство неверно. В общем случае, если подынтегральная функция не определена хотя бы в одном из криволинейных треугольников BEF и CGD рис. 1 из [4] (см. также рис. 1 ниже), то применять лемму 1 из [4] нельзя.

Лемма 1 играет ключевую роль при доказательстве теорем 2 и 3 в [4], но как мы только что видели, пользоваться данной леммой можно не при всех значениях параметров. Для универсальной перестановки местами внешнего и внутреннего интегралов формулировка леммы должна быть скорректирована следующим образом.

Лемма 1. Пусть $\alpha_1 < \beta_1$ – вещественные числа, $l_1(x)$, $l_2(x)$ – две непрерывные монотонно возрастающие функции, $l_1(x) < l_2(x)$ при

$x \in (\alpha_1, \beta_1)$; $\phi(u, v)$ – интегрируемая функция. Тогда имеют место следующие интегральные формулы.

(а) Если $l_1(\beta_1) \leq l_2(\alpha_1)$, то

$$\int_{\alpha_1}^{\beta_1} \int_{l_1(\mu_1)}^{l_2(\mu_1)} \phi(\mu_1, \mu_2) d\mu_2 d\mu_1 = \int_{l_1(\alpha_1)}^{l_1(\beta_1)} \int_{\alpha_1}^{l_1^{-1}(\mu_2)} \phi(\mu_1, \mu_2) d\mu_1 d\mu_2 \\ + \int_{l_1(\beta_1)}^{l_2(\alpha_1)} \int_{\alpha_1}^{\beta_1} \phi(\mu_1, \mu_2) d\mu_1 d\mu_2 + \int_{l_2(\alpha_1)}^{l_2(\beta_1)} \int_{l_2^{-1}(\mu_2)}^{\beta_1} \phi(\mu_1, \mu_2) d\mu_1 d\mu_2.$$

(б) Если $l_1(\beta_1) \geq l_2(\alpha_1)$, то

$$\int_{\alpha_1}^{\beta_1} \int_{l_1(\mu_1)}^{l_2(\mu_1)} \phi(\mu_1, \mu_2) d\mu_2 d\mu_1 = \int_{l_1(\alpha_1)}^{l_2(\alpha_1)} \int_{\alpha_1}^{l_1^{-1}(\mu_2)} \phi(\mu_1, \mu_2) d\mu_1 d\mu_2 \\ + \int_{l_2(\alpha_1)}^{l_1(\beta_1)} \int_{l_2^{-1}(\mu_2)}^{\beta_1} \phi(\mu_1, \mu_2) d\mu_1 d\mu_2 + \int_{l_1(\beta_1)}^{l_2(\beta_1)} \int_{l_1^{-1}(\mu_2)}^{\beta_1} \phi(\mu_1, \mu_2) d\mu_1 d\mu_2.$$

При этом в обоих случаях длины всех внешних промежутков интегрирования в правой части не превосходят

$$\max_{\mu_1 \in [\alpha_1, \beta_1]} (l_2(\mu_1) - \min(l_2(\alpha_1), l_1(\mu_1))). \quad (1)$$

Доказательство. Рассмотрим каждый из случаев (а) и (б) по отдельности (см. рис. 1).

Рис. 1. К лемме 1

Пусть $l_1(\beta_1) \leq l_2(\alpha_1)$. Тогда интеграл в левой части равенства п. (а) равен двукратному интегралу от функции ϕ по криволинейной тра-

пеции $ADFC$ (см. левую часть рис. 1). Эту трапецию можно представить в виде объединения прямоугольника $BDEC$ и двух криволинейных треугольников ABC и DFE . Таким образом, интеграл левой части представляется в виде суммы трех интегралов. Эти интегралы как раз и выписаны в правой части: первый и третий интегралы равны, соответственно, интегралам по криволинейным треугольникам ABC и DFE , а второй интеграл равен интегралу по прямоугольнику $BDEC$. Тем самым интегральное равенство п. (а) доказано.

Для доказательства того, что длины всех внешних промежутков интегрирования в правой части этого равенства не превосходят (1), заметим, что для указанных длин в силу условия $l_1(\beta_1) \leq l_2(\alpha_1)$ и монотонности функций l_1 и l_2 имеют место оценки

$$l_1(\beta_1) - l_1(\alpha_1) \leq l_2(\alpha_1) - l_1(\alpha_1),$$

$$l_2(\beta_1) - l_2(\alpha_1) \leq l_2(\beta_1) - l_1(\beta_1)$$

и

$$l_2(\alpha_1) - l_1(\beta_1) \leq l_2(\beta_1) - l_1(\beta_1).$$

Во всех трех случаях верхняя оценка (1) для длин внешних промежутков интегрирования выполнена.

Пусть $l_1(\beta_1) \geq l_2(\alpha_1)$. Тогда интеграл в левой части равенства п. (b) равен двукратному интегралу от функции ϕ по криволинейной трапеции $ABIG$ (см. правую часть рис. 1). Эту трапецию можно представить в виде объединения криволинейной трапеции $BFGC$ и двух криволинейных треугольников ABC и FIG . Таким образом, интеграл левой части представляется в виде суммы трех интегралов. Эти интегралы как раз и выписаны в правой части: первый и третий интегралы равны, соответственно, интегралам по криволинейным треугольникам ABC и FIG , а второй интеграл равен интегралу по криволинейной трапеции $BFGC$. Тем самым интегральное равенство п. (b) доказано.

Для доказательства того, что длины всех внешних промежутков интегрирования в правой части этого равенства не превосходят (1), заметим, что длины первого и третьего промежутков удовлетворяют оценке тривиальным образом, а для длины второго промежутка в силу условия $l_1(x) < l_2(x)$, $x \in (\alpha_1, \beta_1)$, имеет место неравенство

$$l_1(\beta_1) - l_2(\alpha_1) \leq l_2(\beta_1) - l_2(\alpha_1).$$

Лемма доказана. □

Корректировка формулировки леммы 1 влечет корректировку утверждений теорем 2 и 3 из [4], однако новых формул для функций $G_l^{(1)}$ и $G_l^{(2)}$ с понижением кратности интегрирования здесь не приводим, потому что они слишком громоздки (даже приведенные в теоремах 2 и 3 формулы с учетом всех введенных предварительных обозначений являются весьма громоздкими). Докажем лишь следующую теорему, составляющую один из основных результатов настоящей работы.

Теорема 1. Значения $G_l(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2)$, $l = 2, 3$, при условии $\beta_0 + \beta_1 + (l-1)\beta_2 < 1$ являются суммами не более $10 \cdot 3^{l-1}$ интегралов I_l следующего вида:

$$I_2 = \int_a^b \rho((1-\mu)/\beta_0) \cdot \ln(L(\mu)) \cdot \frac{d\mu}{\mu};$$

$$I_3 = \int_a^b \int_{a_1(\mu_1)}^{b_1(\mu_1)} \rho((1-\mu_1)/\beta_0) \cdot \ln(L_1(\mu_1, \mu_2)) \cdot \frac{d\mu_2}{\mu_2(\mu_1-\mu_2)} d\mu_1,$$

где a и b – вещественные числа, a, a_1, b_1, L, L_1 – линейные функции от переменных интегрирования. Коэффициенты этих линейных функций являются линейными функциями от набора аргументов функций G_l с коэффициентами – абсолютными константами. При этом в промежутках интегрирования значения всех линейных функций $L(\mu)$, μ , $L_1(\mu_1, \mu_2)$, μ_2 , $\mu_1 - \mu_2$, $a_1(\mu_1)$ и $b_1(\mu_1)$ принадлежат отрезку $[\alpha_1; 1 - \beta_0]$ и выполнены неравенства

$$l \cdot \beta_0 < a < b < 1 \quad \text{и} \quad b - a \leq \max(2(\beta_1 - \alpha_1), \beta_2 - \alpha_1). \quad (2)$$

Доказательство. Для понижения кратности интегрирования в интегралах $G_l^{(j)}$ сделаем замену переменных

$$\mu_1 = \lambda_1, \quad \mu_2 = \lambda_1 + \lambda_2, \dots, \mu_l = \lambda_1 + \dots + \lambda_l, \quad (3)$$

позволяющую упростить аргумент функции ρ под знаком интеграла. Тогда

$$G_l^{(1)}(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2) = \frac{1}{(l-1)!} \int_{\alpha_1}^{\beta_1} \int_{\alpha_2+\mu_1}^{\beta_2+\mu_1} \dots \int_{\alpha_2+\mu_{l-1}}^{\beta_2+\mu_{l-1}} \rho\left(\frac{1-\mu_l}{\beta_0}\right) \frac{d\mu_l}{\mu_l-\mu_{l-1}} \dots \frac{d\mu_2}{\mu_2-\mu_1} \frac{d\mu_1}{\mu_1}$$

и

$$G_l^{(2)}(\beta_0, \alpha_1, \beta_1, \beta_2) = \frac{1}{(l-1)!} \int_{\alpha_1}^{\beta_1} \int_{2\mu_1}^{\beta_2+\mu_1} \dots \int_{\mu_1+\mu_{l-1}}^{\beta_2+\mu_{l-1}} \rho\left(\frac{1-\mu_l}{\beta_0}\right) \frac{d\mu_l}{\mu_l-\mu_{l-1}} \dots \frac{d\mu_2}{\mu_2-\mu_1} \frac{d\mu_1}{\mu_1}.$$

Далее рассмотрим отдельно два случая: $l = 2$ и $l = 3$.

Пусть сначала $l = 2$. После перестановки внешнего и внутреннего интегралов согласно равенствам леммы 1 получим, что значения функций $G_2^{(1)}$ и $G_2^{(2)}$ являются суммами трех интегралов вида

$$\int_u^v \int_{l_u(\mu_2)}^{l_v(\mu_2)} \rho\left(\frac{1-\mu_2}{\beta_0}\right) \frac{d\mu_1}{\mu_1(\mu_2-\mu_1)} d\mu_2, \quad (4)$$

где u и v – вещественные числа, а $l_u(\mu_2)$ и $l_v(\mu_2)$ – линейные функции от μ_2 , коэффициенты которых, в свою очередь, являются линейными функциями от входных параметров α_1 , β_1 , α_2 и β_2 . Вычисляя внутренний интеграл в (4), получим, что он равен функции $\rho\left(\frac{1-\mu_2}{\beta_0}\right)$, помноженной на

$$\frac{1}{\mu_2} \cdot \left(\ln\left(\frac{l_v(\mu_2)}{\mu_2 - l_v(\mu_2)}\right) - \ln\left(\frac{l_u(\mu_2)}{\mu_2 - l_u(\mu_2)}\right) \right). \quad (5)$$

Так как $\mu_1 \in [\alpha_1; \beta_1]$ и $\mu_2 - \mu_1 = \lambda_2 \in [\alpha_1; \beta_2]$ в области интегрирования, то значения линейных функций $l_u(\mu_2)$, $l_v(\mu_2)$, $\mu_2 - l_u(\mu_2)$ и $\mu_2 - l_v(\mu_2)$ принадлежат отрезку $[\alpha_1; 1 - \beta_0]$. Следовательно, значения логарифмов определены корректно. Выражение (5) можно представить в виде суммы 4 слагаемых вида $\frac{1}{\mu_2} \cdot \ln(L(\mu_2))$, где L – линейная функция, имеющая вид, указанный в формулировке теоремы. Таким образом, значения функций $G_2^{(1)}$ и $G_2^{(2)}$ являются суммами не более $3 \cdot 4 = 12$ интегралов вида I_2 . Выше мы видели, что числа $G_l(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2)$ равны суммам не более 2 значений функций $G_2^{(1)}$ и $G_2^{(2)}$. Следовательно, эти числа являются суммами не более $24 < 10 \cdot 3^{l-1}$ интегралов вида I_2 . Нам осталось доказать, что для нижнего и верхнего пределов интегрирования a и b интеграла I_2 выполнены неравенства (2).

Согласно лемме 1 имеют место оценки $l_1(\alpha_1) \leq a < b \leq l_2(\beta_1)$, где $l_1(\mu_1)$ и $l_2(\mu_1)$ – линейные функции, являющиеся, соответственно, нижним и верхним пределами интегрирования внутреннего интеграла в равенстве для функции $G_2^{(1)}$ и/или функции $G_2^{(2)}$. Имеем два случая:

- (i) $l_1(\mu_1) = \alpha_2 + \mu_1$, $l_2(\mu_1) = \beta_2 + \mu_1$ в случае функции $G_2^{(1)}$ и
- (ii) $l_1(\mu_1) = 2\mu_1$, $l_2(\mu_1) = \beta_2 + \mu_1$ в случае функции $G_2^{(2)}$. Так как

$$\beta_0 \leq \alpha_1 \quad \text{и} \quad \beta_2 + \mu_1 \leq \beta_2 + \beta_1 < 1 - \beta_0$$

по условию теоремы, то в каждом из случаев (i) и (ii) получим, что $2\beta_0 \leq a < b < 1$, а это и требовалось. Кроме того, значение максимума (1) равно

$$\max_{\mu_1 \in [\alpha_1; \beta_1]} (l_2(\mu_1) - \min(l_2(\alpha_1), l_1(\mu_1))) = \max_{\mu_1 \in [\alpha_1; \beta_1]} \max(\mu_1 - \alpha_1, \beta_2 - \mu_1).$$

Так как последняя величина как раз совпадает с $\beta_2 - \alpha_1$, то при $l = 2$ утверждение теоремы 1 полностью доказано.

Теперь рассмотрим случай $l = 3$. Так как $10 \cdot 3^{l-1} = 36 + 54$, то для доказательства теоремы в этом случае достаточно показать, что значения функции $G_3^{(1)}$ являются суммами не более 36 интегралов вида I_3 , а значения функции $G_3^{(2)}$ являются суммами не более 54 интегралов вида I_3 . Сначала убедимся, что указанное утверждение имеет место для функции $G_3^{(1)}$.

После первой перестановки внешнего и внутреннего интегралов согласно лемме 1 получим, что значения функции $G_3^{(1)}$ являются суммами трех интегралов вида $\int_u^v J_1(\mu_2) \cdot J_2(\mu_2) d\mu_2$, где

$$J_1(\mu_2) = \int_{l_u(\mu_2)}^{l_v(\mu_2)} \frac{d\mu_1}{\mu_1(\mu_2 - \mu_1)}, \quad J_2(\mu_2) = \int_{\alpha_2 + \mu_2}^{\beta_2 + \mu_2} \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2}.$$

Числа u, v и функции $l_u(\mu_2), l_v(\mu_2)$ здесь те же, что и в случае функции $G_2^{(1)}$.

С интегралом $J_1(\mu_2)$ мы уже выше встречались, он равен

$$J_1(\mu_2) = \frac{1}{\mu_2} \cdot \left(\ln\left(\frac{l_v(\mu_2)}{\mu_2 - l_v(\mu_2)}\right) - \ln\left(\frac{l_u(\mu_2)}{\mu_2 - l_u(\mu_2)}\right) \right).$$

Таким образом, значения функции $G_3^{(1)}$ являются суммами не более 12 интегралов вида

$$\int_u^v \int_{\alpha_2 + \mu_2}^{\beta_2 + \mu_2} \phi(\mu_2, \mu_3) d\mu_3 d\mu_2, \quad \phi(\mu_2, \mu_3) = \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \cdot \frac{\ln(L(\mu_2))}{\mu_2(\mu_3 - \mu_2)},$$

где L – линейная функция, имеющая вид, указанный в формулировке теоремы. Вторичная перестановка внешнего и внутреннего интегралов в последнем двойном интеграле приводит к 3 интегралам вида I_3 . Таким образом, суммарно в линейной комбинации имеем не более 36 интегралов вида I_3 .

При рассмотрении случая $l = 2$ было показано, что значения функции L в промежутке интегрирования принадлежат отрезку $[\alpha_1; 1 - \beta_0]$. Так как

$$\mu_2 = \lambda_1 + \lambda_2 \in [\alpha_1 + \alpha_2; \beta_1 + \beta_2], \quad \mu_3 - \mu_2 = \lambda_3 \in [\alpha_2; \beta_2] \quad (6)$$

в области интегрирования и $\beta_0 + \beta_1 + 2\beta_2 < 1$ по условию теоремы, то значения линейных функций μ_2 и $\mu_3 - \mu_2$ принадлежат отрезку $[\alpha_1; 1 - \beta_0]$. По лемме 1 значения линейных функций $a_1(\mu_1)$ и $b_1(\mu_1)$, фигурирующих в описании интеграла I_3 , принадлежат отрезку $[u; v]$.

Учитывая (6), заключаем, что эти значения также принадлежат отрезку $[\alpha_1; 1 - \beta_0]$.

Нам осталось доказать, что для нижнего и верхнего пределов интегрирования a и b интеграла I_3 выполнены неравенства (2).

Согласно лемме 1 для чисел a и b выполнены оценки $\alpha_2 + u \leq a < b \leq \beta_2 + v$. При рассмотрении случая $l = 2$ мы видели, что $2\beta_0 \leq u < v \leq \beta_1 + \beta_2$, поэтому

$$3\beta_0 \leq a < b \leq \beta_1 + 2\beta_2 < 1 - \beta_0.$$

Кроме того, величина (1) удовлетворяет неравенствам

$$\max_{\mu_2 \in [u; v]} (\beta_2 + \mu_2 - \min(\beta_2 + u, \alpha_2 + \mu_2)) = \max(v - u, \beta_2 - \alpha_2).$$

При рассмотрении случая $l = 2$ было показано, что $v - u \leq \beta_2 - \alpha_1$. Следовательно, по лемме 1

$$b - a \leq \max_{\mu_2 \in [u; v]} (\beta_2 + \mu_2 - \min(\beta_2 + u, \alpha_2 + \mu_2)) \leq \beta_2 - \alpha_1,$$

и неравенства (2) доказаны.

Для завершения доказательства теоремы нам осталось рассмотреть случай функции $G_3^{(2)}$. После первой перестановки внешнего и внутреннего интегралов согласно лемме 1 получим, что значения функции $G_3^{(2)}$ являются суммами трех интегралов вида $\int_u^v J_1(\mu_2) \cdot J_2(\mu_1, \mu_2) d\mu_2$, где

$$J_1(\mu_2) = \int_{l_u(\mu_2)}^{l_v(\mu_2)} \frac{d\mu_1}{\mu_1(\mu_2 - \mu_1)}, \quad J_2(\mu_1, \mu_2) = \int_{\mu_1 + \mu_2}^{\beta_2 + \mu_2} \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2}.$$

Числа u, v и функции $l_u(\mu_2), l_v(\mu_2)$ здесь те же, что и в случае функции $G_2^{(2)}$. Однако мы не можем повторить здесь то же рассуждение, что и в рассмотренном выше случае функции $G_3^{(1)}$, потому что интеграл J_2 существенно зависит от переменной μ_1 .

Применим интегрирование по частям $\int F' \Phi d\mu_1 = F\Phi - \int F\Phi' d\mu_1$, полагая

$$F(\mu_1) = \frac{1}{\mu_2} \ln \frac{\mu_1}{\mu_2 - \mu_1} \quad \text{и} \quad \Phi(\mu_1) = \int_{\mu_1 + \mu_2}^{\beta_2 + \mu_2} \frac{\rho((1 - \mu_3)/\beta_0) d\mu_3}{\mu_3 - \mu_2}.$$

Тогда $\partial F(\mu_1)/\partial \mu_1 = \frac{1}{\mu_1(\mu_2 - \mu_1)}$ и

$$\begin{aligned} & \int_{l_u(\mu_2)}^{l_v(\mu_2)} \int_{\mu_1 + \mu_2}^{\beta_2 + \mu_2} \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2} \frac{d\mu_1}{\mu_1(\mu_2 - \mu_1)} \\ &= \left(\frac{1}{\mu_2} \ln \frac{\mu_1}{\mu_2 - \mu_1} \cdot \int_{\mu_1 + \mu_2}^{\beta_2 + \mu_2} \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2} \right) \Big|_{\mu_1 = l_u(\mu_2)}^{\mu_1 = l_v(\mu_2)} \\ & \quad + \int_{l_u(\mu_2)}^{l_v(\mu_2)} \frac{1}{\mu_2} \cdot \ln \frac{\mu_1}{\mu_2 - \mu_1} \cdot \rho\left(\frac{1 - \mu_1 - \mu_2}{\beta_0}\right) \frac{d\mu_1}{\mu_1}. \end{aligned}$$

В последнем интеграле сделаем замену переменной $\mu_3 = \mu_1 + \mu_2$. Тогда получим

$$\begin{aligned} & \int_{l_u(\mu_2)}^{l_v(\mu_2)} \int_{\mu_1 + \mu_2}^{\beta_2 + \mu_2} \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2} \frac{d\mu_1}{\mu_1(\mu_2 - \mu_1)} \\ &= \left(\frac{1}{\mu_2} \ln \frac{\mu_1}{\mu_2 - \mu_1} \cdot \int_{\mu_1 + \mu_2}^{\beta_2 + \mu_2} \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2} \right) \Big|_{\mu_1 = l_u(\mu_2)}^{\mu_1 = l_v(\mu_2)} \\ & \quad + \int_{l_u(\mu_2) + \mu_2}^{l_v(\mu_2) + \mu_2} \frac{1}{\mu_2} \cdot \ln \frac{\mu_3 - \mu_2}{2\mu_2 - \mu_3} \cdot \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2}. \quad (7) \end{aligned}$$

В правой части равенства (7) стоит сумма трех интегралов вида

$$\int_{g_1(\mu_2)}^{g_2(\mu_2)} \frac{1}{\mu_2} \cdot \ln \frac{L'(\mu_2, \mu_3)}{L''(\mu_2, \mu_3)} \cdot \rho\left(\frac{1 - \mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3 - \mu_2},$$

где g_1 , g_2 , L' и L'' – линейные функции, коэффициенты которых, в свою очередь, являются линейными функциями от входных параметров α_1 , β_1 , α_2 и β_2 . Значения линейных функций $L'(\mu_2, \mu_3)$, $L''(\mu_2, \mu_3)$, μ_2 и $\mu_3 - \mu_2$ принадлежат отрезку $[\alpha_1; 1 - \beta_0]$ в области интегрирования. Действительно, по отношению к функции μ_2 это ясно. Разность $\mu_3 - \mu_2$ в силу сделанных выше замен переменных равна либо λ_3 , либо λ_1 (в зависимости от интеграла). В любом случае она принадлежит указанному отрезку. Значения линейных функций $l_u(\mu_2)$, $l_v(\mu_2)$, $\mu_2 - l_u(\mu_2)$ и $\mu_2 - l_v(\mu_2)$ принадлежат отрезку $[\alpha_1; 1 - \beta_0]$ в силу тех же аргументов, которые приводились при рассмотрении случая $l = 2$. Наконец, линейная функция $2\mu_2 - \mu_3$ равна $\mu_2 - \mu_1 = \lambda_2$, т. е. ее значения также принадлежат рассматриваемому отрезку.

Таким образом, значения функции $G_3^{(2)}$ являются суммами не более 18 интегралов вида

$$\int_u^v \int_{g_1(\mu_2)}^{g_2(\mu_2)} \frac{1}{\mu_2} \cdot \ln(L_1(\mu_2, \mu_3)) \cdot \rho\left(\frac{1-\mu_3}{\beta_0}\right) \frac{d\mu_3}{\mu_3-\mu_2} d\mu_2,$$

где L_1 – линейная функция, имеющая вид, указанный в формулировке теоремы. Вторичная перестановка внешнего и внутреннего интегралов в последнем двойном интеграле приводит к 3 интегралам вида I_3 . Таким образом, суммарно в линейной комбинации имеем не более 54 интегралов вида I_3 . Значения линейных функций $a_1(\mu_1)$ и $b_1(\mu_1)$, фигурирующих в описании этих интегралов, принадлежат отрезку $[\alpha_1; 1 - \beta_0]$ в силу тех же аргументов, которые приводились при рассмотрении функции $G_3^{(1)}$.

Нам осталось доказать, что нижний и верхний пределы интегрирования a и b интеграла I_3 , определенные описанным выше образом, удовлетворяют неравенствам (2).

Согласно лемме 1 (с соответствующей переменной обозначений), числа a и b являются значениями функции g_1 и/или g_2 в точке u и/или v , поэтому для них выполнены оценки $g_1(u) \leq a < b \leq g_2(v)$. Ввиду равенства (7) для чисел $g_1(u)$ и $g_2(v)$ справедливы оценки

$$g_1(u) = \min_{\mu_2 \in [u; v]} g_1(\mu_2) \geq \min_{\substack{\mu_1 \in [\alpha_1; \beta_1], \\ \mu_2 \in [u; v]}} (\mu_1 + \mu_2) = \alpha_1 + u,$$

$$g_2(v) = \max_{\mu_2 \in [u; v]} g_2(\mu_2) \leq \max_{\mu_2 \in [u; v]} (\beta_2 + \mu_2) = \beta_2 + v.$$

При рассмотрении случая $l = 2$ мы видели, что $2\beta_0 \leq u < v \leq \beta_1 + \beta_2$, поэтому

$$3\beta_0 \leq a < b \leq \beta_1 + 2\beta_2 < 1 - \beta_0.$$

Этим доказана часть неравенств (2). Для доказательства теоремы осталось доказать лишь оценку

$$b - a \leq \max(2(\beta_1 - \alpha_1), \beta_2 - \alpha_1). \quad (8)$$

Согласно доказательству леммы 1 разность $b - a$ не превосходит

$$\max_{\mu_2 \in [u; v]} (g_2(\mu_2) - g_1(\mu_2))$$

во всех случаях, за возможным исключением второго слагаемого правой части равенства в условии (b) леммы. Для этого конкретного слагаемого разность $b - a$ равна $g_1(v) - g_2(u)$. Так как

$$g_2(\mu_2) \leq \beta_2 + \mu_2 \quad \text{и} \quad g_1(\mu_2) \geq l_u(\mu_2) + \mu_2 \geq \alpha_1 + \mu_2,$$

то $g_2(\mu_2) - g_1(\mu_2) \leq \beta_2 - \alpha_1$ и оценка (8) выполнена. Таким образом, для доказательства теоремы осталось доказать лишь оценку

$$g_1(v) - g_2(u) \leq \max(2(\beta_1 - \alpha_1), \beta_2 - \alpha_1). \quad (9)$$

Функция $g_2(t)$ равна либо $\beta_2 + t$, либо $l_v(t) + t$. В первом случае имеем

$$g_1(v) - g_2(u) \leq g_2(v) - g_2(u) = v - u \leq \beta_2 - \alpha_1$$

по доказанному при рассмотрении случая $l = 2$. Таким образом, в первом случае неравенство (9) доказано.

Во втором случае функция $g_1(t)$ равна $l_u(t) + t$. Далее, учитывая, что $l_1(\mu_1) = 2\mu_1$ и $l_2(\mu_1) = \beta_2 + \mu_1$, где $l_1(\mu_1)$ и $l_2(\mu_1)$ – линейные функции, являющиеся, соответственно, нижним и верхним пределами интегрирования по переменной μ_2 в равенстве для функции $G_3^{(2)}$, имеем два случая: (а) $l_v(t) = \beta_1$ и (б) $l_v(t) = t/2$. В случае (а) разность $g_2(v) - g_2(u)$ снова совпадает с $v - u$, поэтому неравенство (9) выполняется. В случае (б) возможны два случая:

$$(b') \quad u = l_1(\alpha_1), \quad v \leq l_1(\beta_1), \quad l_u(t) = \alpha_1, \quad l_v(t) = t/2,$$

$$(b'') \quad u = l_2(\alpha_1), \quad v = l_1(\beta_1), \quad l_u(t) = t - \beta_2, \quad l_v(t) = t/2.$$

В случае (b')

$$g_1(v) - g_2(u) = \alpha_1 + v - \frac{3}{2} \cdot 2\alpha_1 \leq 2(\beta_1 - \alpha_1).$$

В случае (b'')

$$g_1(v) - g_2(u) = 2v - \beta_2 - \frac{3}{2} \cdot (\beta_2 + \alpha_1) = 4 \cdot \beta_1 - 2.5 \cdot \beta_2 - 1.5 \cdot \alpha_1.$$

Так как последняя разность не превосходит $1.5 \cdot (\beta_1 - \alpha_1)$, то оценка (9) во всех случаях выполняется. Теорема доказана. $\square$

3. Алгоритмы вычисления интегралов

Как известно [6], функция Дикмана $\rho(x)$ имеет особенности в целых точках $k = 0, 1, 2, \dots$. На любом отрезке $[k - 1; k]$ она совпадает с аналитической функцией, задаваемой рядом Тейлора с радиусом сходимости 1. Обозначим последнюю через $\rho_k(x)$. В [3] был предложен алгоритм быстрого вычисления коэффициентов $c_{k,i}$ разложения

$$\rho_k(k - 0.5 - x) = \sum_{i \geq 0} c_{k,i} \cdot x^i, \quad -0.5 \leq x \leq 0.5, \quad k = 1, 2, \dots, \quad (10)$$

функции Дикмана в ряды Тейлора в полуцелых точках. Этим разложением, а также доказанной в [3] оценкой

$$0 \leq c_{k,i} \leq 1.5^{-i}, \quad i \geq 0, \quad k \geq 1, \quad (11)$$

будем пользоваться и в настоящей работе.

Сначала займемся вычислением интеграла I_2 теоремы 1. Пусть $\theta_k = 1 - k/\beta_0$ и $\lambda_k = 1 - (k - 0.5)\beta_0$, $k = 0, 1, \dots$. Тогда $\lceil (1 - \mu)/\beta_0 \rceil = k$ при $\mu \in [\theta_k; \theta_{k-1})$. Следовательно,

$$\rho\left(\frac{1-\mu}{\beta_0}\right) = \rho_k\left(\frac{1-\mu}{\beta_0}\right) = \sum_{i \geq 0} c_{k,i} x^i, \quad x = k - 0.5 - \frac{1-\mu}{\beta_0} = \frac{\mu}{\beta_0} - \frac{\lambda_k}{\beta_0}.$$

Введем в рассмотрение следующие две величины:

$$k_\mu = \max(k : \theta_k > \mu) = \lceil \frac{1-\mu}{\beta_0} \rceil - 1, \quad K_\mu = \min(k : \theta_k < \mu) = \lfloor \frac{1-\mu}{\beta_0} \rfloor + 1.$$

Тогда имеем два случая.

(1) На интервале $(\frac{1-b}{\beta_0}; \frac{1-a}{\beta_0})$ нет целых точек. Тогда $k_a = K_b - 1$ и

$$I_2 = \int_a^b \rho_k((1-\mu)/\beta_0) \cdot \ln(L(\mu)) \frac{d\mu}{\mu}, \quad k = K_b.$$

(2) На интервале $(\frac{1-b}{\beta_0}; \frac{1-a}{\beta_0})$ есть целые точки. Тогда $k_a \geq K_b$ и

$$\begin{aligned} I_2 = & \int_a^{\theta_{k_a}} \rho_{k_a+1}((1-\mu)/\beta_0) \cdot \ln(L(\mu)) \frac{d\mu}{\mu} \\ & + \int_{\theta_{K_b}}^b \rho_{K_b}((1-\mu)/\beta_0) \cdot \ln(L(\mu)) \frac{d\mu}{\mu} \\ & + \sum_{K_b+1 \leq k \leq k_a} \int_{\theta_k}^{\theta_{k-1}} \rho_k((1-\mu)/\beta_0) \cdot \ln(L(\mu)) \frac{d\mu}{\mu}. \end{aligned}$$

Таким образом, интеграл I_2 является линейной комбинацией интегралов вида

$$F_2 = \int_A^B \rho_k((1-\mu)/\beta_0) \cdot \ln(L(\mu)) \frac{d\mu}{\mu}, \quad (12)$$

где A и B – пределы интегрирования, удовлетворяющие условию

$$(1-\mu)/\beta_0 \in [k-1; k], \quad \text{если } \mu \in [A; B]. \quad (13)$$

Из (13) следует, что

$$(1-\mu)/\beta_0 = k - 0.5 - x, \quad -0.5 \leq x \leq 0.5. \quad (14)$$

Выражая x через μ , получим

$$x = k - 0.5 - \frac{1-\mu}{\beta_0} = \frac{\mu}{\beta_0} - \frac{\lambda_k}{\beta_0}, \quad \lambda_k = 1 - \beta_0 \cdot (k - 0.5). \quad (15)$$

Используя разложение (10) и формулы (14) и (15), запишем интеграл и F_2 в виде

$$F_2 = \int_A^B \sum_{i \geq 0} c_{k,i} \cdot \left(\frac{\mu}{\beta_0} - \frac{\lambda_k}{\beta_0}\right)^i \cdot \ln(L(\mu)) \frac{d\mu}{\mu}.$$

Переставляя знаки сумм и интегралов и делая замену переменной

$$t = \mu/\beta_0, \quad u = A/\beta_0, \quad v = B/\beta_0, \quad w = \lambda_k/\beta_0,$$

придем к формуле

$$F_2 = \sum_{i \geq 0} c_{k,i} \cdot F_2^{(i)}, \quad F_2^{(i)} = \int_u^v (t-w)^i \cdot \ln(L_1(t)) \cdot \frac{dt}{t}, \quad (16)$$

где $L_1(t) = L(\beta_0 t)$. В силу (14) и (15) в этой формуле имеет место оценка $|t-w| \leq 0.5$ при любом $t \in [u, v]$. Сомножитель $\ln(L_1(t))/t$ ограничен, так как по теореме 1 $u = A/\beta_0 \geq 2$ и $L(\mu) \geq \alpha_1$. При вычислении суммы (16) можно ограничиться значениями $i \leq 50$, так как ввиду (11) и неравенства $|t-w| \leq 0.5$ вклад остальных слагаемых в сумму (16) будет слишком мал по сравнению с погрешностью стандартного типа `double` (тип `double` в языке программирования C++ имеет 53-битовую мантиссу).

Линейную функцию $L_1(t)$ можно представить либо в виде $c \cdot (t-w_2)$, либо в виде $c \cdot (w_2 - t)$, где $c > 0$. Поэтому интеграл $F_2^{(i)}$ представляет собой линейную комбинацию интегралов

$$J_{1,1}^{(i)} = \int_u^v \frac{(t-w)^i}{t-w_1} dt, \quad (17)$$

$$J_{2,1}^{(i)} = \int_u^v \frac{(t-w)^i \cdot \ln(t-w_2)}{t-w_1} dt \quad (18)$$

и

$$\bar{J}_{2,1}^{(i)} = \int_u^v \frac{(t-w)^i \cdot \ln(w_2-t)}{t-w_1} dt. \quad (19)$$

В разделах 5.2.1 и 5.2.3 работы [3] предложены эффективные алгоритмы вычисления интегралов (17) и (18). Вычисление интеграла (19) проводится методом, полностью аналогичным методу из [3]. Этим исчерпывается вопрос о вычислении интеграла I_2 теоремы 1.

Вычисление интеграла I_3 проводится в несколько этапов. Сначала покажем, как эффективно вычислять более простые интегралы следующих видов:

$$J_{3,1}^{(i)}(u, v, w) = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{(t_1-w)^i}{t_2(t_1-t_2)} dt_2 dt_1, \quad (20)$$

$$J_{3,2}^{(i)}(u, v, w) = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{(t_1-w)^i \cdot t_1}{t_2(t_1-t_2)} dt_2 dt_1, \quad (21)$$

$$F_3 = \int_A^B \int_{l_1(\mu_1)}^{l_2(\mu_1)} \rho_k((1-\mu_1)/\gamma) \cdot \ln(L(\mu_1, \mu_2)) \cdot \frac{d\mu_2 d\mu_1}{\mu_2(\mu_1-\mu_2)}. \quad (22)$$

В этих формулах величины $u - w$ и $v - w$ в дальнейшем всегда будут равны некоторому значению x в разложении (10). Поэтому в описываемых ниже алгоритмах предполагается, что выполнена оценка

$$\max(|u - w|, |v - w|) \leq 0.5. \quad (23)$$

Также предполагается, что $w > 1$. Буквами l_1 , l_2 и L обозначены линейные функции от переменных интегрирования. Предполагается, что значения функции L принадлежат отрезку $[\alpha_1; 1 - \beta_0]$, а значения линейных функций l_1 , l_2 , t_2 и $t_1 - t_2$ не меньше 1. Для сокращения записи последующих формул будем опускать указание набора параметров интеграла там, где этот набор ясен из контекста.

Ниже увидим, что интеграл I_3 вычисляется через интегралы вида (22), а последние вычисляются через интегралы (20) и (21). Поэтому начнем с описания алгоритмов быстрого вычисления интегралов (20) и (21).

3.1. Алгоритмы вычисления значений $J_{3,2}^{(i)}$ и $J_{3,1}^{(i)}$

Начнем с того, что сначала покажем, как вычислять значения интеграла

$$\int_u^v \ln(L_1(t)) \cdot \frac{dt}{L_2(t)}, \quad (24)$$

где u и v – вещественные числа, а L_1 и L_2 – линейные функции от переменной интегрирования t . Рассмотрим несколько случаев. Если $L_1(t)$ и $L_2(t)$ – тождественные константы, то вычислять ничего не надо. Если ровно одна из этих функций – тождественная константа, то вычисление интеграла тривиально. Пусть обе функции существенно зависят от t : $L_1(t) = a_{1,1}t + a_{1,2}$ и $L_2(t) = a_{2,1}t + a_{2,2}$, где $a_{1,1}a_{2,1} \neq 0$. Сделаем замену переменной $s = \epsilon \cdot L_2(t)$, где $\epsilon = \text{sgn}(a_{1,1}a_{2,1})$. Тогда интеграл (24) примет вид

$$(1/a_{2,1}) \cdot \int_{\epsilon \cdot L_2(u)}^{\epsilon \cdot L_2(v)} \ln(L_3(s)) \cdot \frac{ds}{s}, \quad (25)$$

где $L_3 = a_{3,1}t + a_{3,2}$ – линейная функция от переменной интегрирования s , причем $a_{3,1} = \epsilon \cdot a_{1,1}/a_{2,1} > 0$. Алгоритм вычисления интеграла (25) приведен в [3, п. 5.2.2]. На этом описание метода вычисления интеграла (24) закончено.

Теперь перейдем к рассмотрению интегралов (20) и (21). Используя равенство $\frac{t_1}{t_2(t_1 - t_2)} = \frac{1}{t_2} + \frac{1}{t_1 - t_2}$, запишем интеграл $J_{3,2}^{(i)}$ в виде суммы двух интегралов

$$J_{3,2}^{(i)} = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{(t_1 - w)^i}{t_2} dt_2 dt_1$$

$$+ \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{(t_1-w)^i}{t_1-t_2} dt_2 dt_1.$$

Интегрируя по частям каждый из интегралов в правой части, получим, что $J_{3,2}^{(i)} = A_1 - B_1$, где

$$A_1 = \frac{(t_1-w)^{i+1}}{i+1} \cdot \left(\int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{dt_2}{t_2} + \int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{dt_2}{t_1-t_2} \right) \Big|_{t_1=u}^{t_1=v},$$

$$B_1 = \int_u^v \frac{(t_1-w)^{i+1}}{i+1} \cdot \frac{d}{dt_1} \left(\int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{dt_2}{t_2} + \int_{l_1(t_1)}^{l_2(t_1)} \ln(L(t_1, t_2)) \cdot \frac{dt_2}{t_1-t_2} \right) dt_1.$$

Величина A_1 представляет собой линейную комбинацию интегралов вида (24). Вычисляя производную в выражении для B_1 , получим, что $B_1 = B_{1,1} + B_{1,2} + B_{1,3}$, где

$$B_{1,1} = \int_u^v \frac{(t_1-w)^{i+1}}{i+1} \cdot \left(\ln(L(t_1, l_2(t_1))) \cdot \frac{l_2'(t_1)}{l_2(t_1)} - \ln(L(t_1, l_1(t_1))) \cdot \frac{l_1'(t_1)}{l_1(t_1)} \right) dt_1,$$

$$B_{1,2} = \int_u^v \frac{(t_1-w)^{i+1}}{i+1} \cdot \left(\ln(L(t_1, l_2(t_1))) \cdot \frac{l_2'(t_1)}{t_1-l_2(t_1)} - \ln(L(t_1, l_1(t_1))) \cdot \frac{l_1'(t_1)}{t_1-l_1(t_1)} \right) dt_1,$$

$$B_{1,3} = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \left(\frac{(\partial/\partial t_1)L(t_1, t_2)}{L(t_1, t_2)} \cdot \left(\frac{1}{t_2} + \frac{1}{t_1-t_2} \right) - \frac{\ln(L(t_1, t_2))}{(t_1-t_2)^2} \right) \cdot \frac{(t_1-w)^{i+1}}{i+1} dt_2 dt_1.$$

Интегралы $B_{1,1}$ и $B_{1,2}$ – линейные комбинации интегралов вида

$$H^{(i+1)} = \int_u^v (t-w)^{i+1} \cdot \ln(l_3(t)) \cdot \frac{dt}{l_4(t)}, \quad (26)$$

где l_3 и l_4 – линейные функции от t . При этом отношение $\frac{\ln(l_3(t))}{l_4(t)}$ ограничено при $t \in [u; v]$, так как значения функции L принадлежат отрезку $[\alpha_1; 1 - \beta_0]$, а значения функций l_1 и l_2 не меньше 1 по предположению. Функцию l_3 можно представить либо в виде $c \cdot (t - w_2)$, либо в виде $c \cdot (w_2 - t)$, где $c > 0$. Поэтому интеграл $H^{(i)}$ является линейной комбинацией интегралов видов (17), (18) и (19), алгоритмы вычисления которых были упомянуты в предыдущем разделе. Этим исчерпывается вопрос о вычислении интегралов $B_{1,1}$ и $B_{1,2}$.

Нам осталось вычислить интеграл $B_{1,3}$. Представим его в виде $B_{1,3} = C_1 + C_2 - C_3$, где

$$C_1 = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \frac{(\partial/\partial t_1)L(t_1, t_2)}{L(t_1, t_2)} \cdot \frac{1}{t_2} \cdot \frac{(t_1-w)^{i+1}}{i+1} dt_2 dt_1,$$

$$C_2 = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \frac{(\partial/\partial t_1)L(t_1, t_2)}{L(t_1, t_2)} \cdot \frac{1}{t_1-t_2} \cdot \frac{(t_1-w)^{i+1}}{i+1} dt_2 dt_1,$$

$$C_3 = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \frac{\ln(L(t_1, t_2))}{(t_1-t_2)^2} \cdot \frac{(t_1-w)^{i+1}}{i+1} dt_2 dt_1.$$

При вычислении интегралов C_1 и C_2 можно считать, что $(\partial/\partial t_1) L \neq 0$, т. е. L существенно зависит от переменной t_1 . Если $(\partial/\partial t_2) L = 0$, то

$$C_1 + C_2 = \int_u^v \frac{(t_1-w)^{i+1}}{i+1} \cdot \left(\frac{(\partial/\partial t_1) L}{L} \cdot \ln\left(\frac{t_2}{t_1-t_2}\right) \Big|_{t_2=l_1(t_1)}^{t_2=l_2(t_1)} \right) dt_1.$$

Отсюда видно, что сумма $C_1 + C_2$ представляется в виде линейной комбинации интегралов вида (26), а потому может быть вычислена способом, указанным выше. Пусть $(\partial/\partial t_2) L \neq 0$, т. е. L существенно зависит от переменной t_2 . Сначала рассмотрим случай $L(t_1, t_2) = c_2(t_1 - t_2)$, где $c_2 \neq 0$ – некоторая константа. Тогда имеет место представление

$$\frac{1}{L(t_1, t_2)} \cdot \left(\frac{1}{t_2} + \frac{1}{t_1-t_2} \right) = \frac{1}{c_2 t_1} \cdot \left(\frac{1}{t_1-t_2} + \frac{1}{t_2} \right) + \frac{1}{c_2(t_1-t_2)^2}.$$

В этом случае

$$\begin{aligned} & C_1 + C_2 \\ &= \int_u^v \frac{(t_1-w)^{i+1}}{i+1} \cdot \frac{1}{c_2 t_1} \cdot \ln\left(\frac{t_2}{t_1-t_2}\right) \Big|_{t_2=l_1(t_1)}^{t_2=l_2(t_1)} dt_1 + \int_u^v \frac{(t_1-w)^{i+1}}{i+1} \cdot \frac{1}{c_2(t_1-t_2)} \Big|_{t_2=l_1(t_1)}^{t_2=l_2(t_1)} dt_1. \end{aligned}$$

Отсюда видно, что сумма $C_1 + C_2$ представляется в виде линейной комбинации интегралов вида (26), а также интегралов $J_{1,1}^{(i+1)}$, определенных формулой (17) с заменой индекса i на $i+1$. Таким образом, сумма $C_1 + C_2$ может быть вычислена указанными выше методами.

Для окончательного вычисления значения интеграла $J_{3,2}^{(i)}$ осталось вычислить двойной интеграл C_3 . Используя интегрирование по частям, представим его в виде $C_3 = C_{3,1} - C_{3,2}$, где

$$C_{3,1} = \int_u^v \frac{(t_1-w)^{i+1}}{i+1} \cdot \frac{\ln(L(t_1, t_2))}{t_1-t_2} \Big|_{t_2=l_1(t_1)}^{t_2=l_2(t_1)} dt_1,$$

$$C_{3,2} = \int_u^v \int_{l_1(t_1)}^{l_2(t_1)} \frac{(\partial/\partial t_2) L(t_1, t_2)}{L(t_1, t_2)} \cdot \frac{1}{t_1-t_2} \cdot \frac{(t_1-w)^{i+1}}{i+1} dt_2 dt_1.$$

Интеграл $C_{3,1}$ представляется в виде линейной комбинации интегралов вида (26), а потому может быть вычислен способом, указанным выше. Интеграл $C_{3,2}$ лишь постоянным множителем отличается от интеграла C_2 , а потому может быть вычислен способом, указанным выше. На этом описание метода вычисления интеграла (21) закончено.

Для интеграла (20) имеет место рекуррентная формула

$$J_{3,1}^{(i)} = J_{3,2}^{(i-1)} - w \cdot J_{3,1}^{(i-1)}, \quad i = 1, 2, \dots, 60. \quad (27)$$

Перепишем ее в обратном направлении, т. е.

$$J_{3,1}^{(i-1)} = (J_{3,2}^{(i-1)} - J_{3,1}^{(i)})/w, \quad i = 60, 59, \dots, 1. \quad (28)$$

Так как $w > 1$ по предположению, то для вычисления интегралов (20) предлагается использовать формулу (28), установив стартовое значение $J_{3,1}^{(60)} = 0$. Вычислительные эксперименты показывают, что при таком способе вычислений не будет происходить экспоненциального роста ошибки округления, как это было бы при прямом порядке (27). Стартовое значение $i_0 = 60$ установлено по тем же соображениям, что и выше: ввиду неравенства $|t_1 - w| \leq 0.5$ значения остальных интегралов будут слишком малы по сравнению с погрешностью стандартного типа `double` (53 бита мантиссы).

Также отметим, что в [3] была выбрана неоправданно большая граница 1075 вместо 60 для числа i_0 . Это привело к значительной потере скорости вычисления значений функций G_l , $l = 2, 3$. За счет уменьшения величины i_0 до 60 (а при уменьшении точности вычислений можно обойтись и еще меньшей границей) время вычисления значений функций G_l может быть сделано в десятки раз меньше тех чисел, которые приведены в последнем столбце таблицы 1 из [3, раздел 4]. Тогда предложенный в [3] специализированный алгоритм окажется во всех случаях быстрее, чем рассмотренные в [3, раздел 4] альтернативные методы вычисления значений кратных интегралов.

3.2. Алгоритм вычисления значения F_3

В данном разделе покажем, как быстро вычислить интеграл (22), где a_1 , b_1 и L_1 – линейные функции из формулировки теоремы 1, в частности значения всех линейных функций $L_1(\mu_1, \mu_2)$, μ_2 , $\mu_1 - \mu_2$, $a_1(\mu_1)$ и $b_1(\mu_1)$ принадлежат отрезку $[\alpha_1; 1 - \beta_0]$ в промежутках интегрирования. Также предполагается, что пределы интегрирования A и B удовлетворяют оценке $l \cdot \beta_0 \leq A < B < 1$ и условию (13). Используя разложение (10) и формулы (14) и (15), вытекающие из условия (13), запишем интеграл F_3 в виде

$$F_3 = \int_A^B \int_{a_1(\mu_1)}^{b_1(\mu_1)} \sum_{i \geq 0} c_{k,i} \cdot \left(\frac{\mu_1}{\beta_0} - \frac{\lambda_k}{\beta_0} \right)^i \cdot \frac{\ln(L_1(\mu_1, \mu_2))}{\mu_2(\mu_1 - \mu_2)} d\mu_2 d\mu_1.$$

Переставляя знаки сумм и интегралов и делая замену переменных

$$t_1 = \mu_1/\beta_0, \quad t_2 = \mu_2/\beta_0, \quad u = A/\beta_0, \quad v = B/\beta_0, \quad w = \lambda_k/\beta_0,$$

придем к формуле

$$F_3 = \sum_{i \geq 0} c_{k,i} \cdot F_3^{(i)}, \quad F_3^{(i)} = \int_u^v \cdot \int_{a_2(t_1)}^{b_2(t_1)} \frac{\ln(L_2(t_1, t_2))}{t_2(t_1 - t_2)} \cdot (t_1 - w)^i dt_2 dt_1, \quad (29)$$

где

$$a_2(t_1) = \frac{a_1(\beta_0 t_1)}{\beta_0}, \quad b_2(t_1) = \frac{b_1(\beta_0 t_1)}{\beta_0} \quad \text{и} \quad L_2(t_1, t_2) = L_1(\beta_0 t_1, \beta_0 t_2).$$

В силу (14) и (15) в формуле (29) имеет место оценка $|t_1 - w| \leq 0.5$ при любом $t_1 \in [u; v]$. Сомножитель $\frac{\ln(L_2(\beta_0 t_1, \beta_0 t_2))}{t_2(t_1 - t_2)}$ ограничен ввиду того, что значения линейных функций $L_1(\mu_1, \mu_2)$, μ_2 , $\mu_1 - \mu_2$ принадлежат отрезку $[\alpha_1; 1 - \beta_0]$ по теореме 1. Из оценок (11) и $|t_1 - w| \leq 0.5$ следует, что при суммировании можно ограничиться значениями $i \leq 50$, так как вклад остальных слагаемых в сумму (29) будет слишком мал по сравнению с погрешностью типа **double**.

Так как

$$\frac{A}{\beta_0} \geq l = 3 \quad \text{и} \quad \frac{1-B}{\beta_0} = \min_{\mu_1 \in [A; B]} \left(\frac{1-\mu_1}{\beta_0} \right) \geq k - 1$$

в силу предположений, то

$$w = \frac{\lambda_k}{\beta_0} = \frac{1}{\beta_0} - k + 0.5 \geq \frac{B}{\beta_0} - 0.5 \geq \frac{A}{\beta_0} - 0.5 \geq 2.5.$$

Это показывает, что интеграл $F_3^{(i)}$ является частным случаем интеграла $J_{3,1}^{(i)}$, алгоритм вычисления которого был описан в предыдущем разделе. Применяя этот алгоритм и вычисляя сумму (29), получим значение интеграла F_3 .

3.3. Алгоритм вычисления значения I_3

Покажем, как вычислить интеграл I_3 теоремы 1. Пусть величины θ_k , λ_k , k_μ и K_μ определены так же, как и в разделе 3. Тогда имеем два случая.

(1) На интервале $(\frac{1-b}{\beta_0}; \frac{1-a}{\beta_0})$ нет целых точек. Тогда $k_a = K_b - 1$ и

$$I_3 = \int_a^b \int_{a_1(\mu_1)}^{b_1(\mu_1)} \ln(L_1(\mu_1, \mu_2)) \cdot \rho_k((1 - \mu_1)/\beta_0) \cdot \frac{d\mu_2 d\mu_1}{\mu_2(\mu_1 - \mu_2)}, \quad k = K_b.$$

(2) На интервале $(\frac{1-b}{\beta_0}; \frac{1-a}{\beta_0})$ есть целые точки. Тогда $k_a \geq K_b$ и

$$\begin{aligned} I_3 = & \int_a^{\theta_{k_a}} \int_{a_1(\mu_1)}^{b_1(\mu_1)} \ln(L_1(\mu_1, \mu_2)) \cdot \rho_{k_a+1}((1 - \mu_1)/\beta_0) \cdot \frac{d\mu_2 d\mu_1}{\mu_2(\mu_1 - \mu_2)} \\ & + \int_{\theta_{K_b}}^b \int_{a_1(\mu_1)}^{b_1(\mu_1)} \ln(L_1(\mu_1, \mu_2)) \cdot \rho_{K_b}((1 - \mu_1)/\beta_0) \cdot \frac{d\mu_2 d\mu_1}{\mu_2(\mu_1 - \mu_2)} \\ & + \sum_{K_b+1 \leq k \leq k_a} \int_{\theta_k}^{\theta_{k-1}} \int_{a_1(\mu_1)}^{b_1(\mu_1)} \ln(L_1(\mu_1, \mu_2)) \cdot \rho_k((1 - \mu_1)/\beta_0) \cdot \frac{d\mu_2 d\mu_1}{\mu_2(\mu_1 - \mu_2)}. \end{aligned}$$

Таким образом, интеграл I_3 является линейной комбинацией интегралов вида F_3 из предыдущего раздела. Применяя изложенный выше алгоритм вычисления этих интегралов, получим метод вычисления интеграла I_3 , а следовательно, и значений $G_l(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2)$ при $l = 2, 3$.

4. Трудоемкость методов

Пусть $n = \lceil \frac{\max_i \beta_i}{\beta_0} \rceil + 1$. Как следует из [4], значения

$$G_2(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2), G_3(\beta_0, \alpha_1, \beta_1, \alpha_2, \beta_2) \quad (30)$$

являются суммами $O(1)$ значений интегралов видов I_2 и I_3 из теоремы 1. Ввиду оценки (2) теоремы 1 и описания методов, изложенных в предыдущих разделах, интегралы I_2 и I_3 являются суммами $O(n)$ значений (12) и (22), поэтому, для вычисления значений (30) с абсолютной погрешностью δ достаточно вычислить все встречающиеся значения (12) и (22) с абсолютной погрешностью $\delta/(c_0 \cdot n)$, где $c_0 \geq 1$ – константа.

В свою очередь, значения (12) и (22) являются суммами рядов, элементы которых (обозначим их через $a_{k,i}$) являются линейными комбинациями интегралов (17), (18), (19) и (20), которые будем для краткости называть интегралами типа J . В силу оценки (11) с ростом индекса i элементы $a_{k,i}$ убывают по абсолютной величине со скоростью геометрической прогрессии равномерно по всем $k \leq n$. Поэтому, чтобы вычислить сумму такого ряда с абсолютной погрешностью δ_1 , достаточно учесть лишь $O(\ln \delta_1)$ первых членов ряда. Это показывает, что для вычисления значений (30) с фиксированной абсолютной погрешностью достаточно вычислить $O(n \ln n)$ интегралов типа J .

Следует отметить, что согласно леммам 1, 2 и 4 в [3] вычисление коэффициентов $c_{k,i}$ разложения (10), необходимых для вычисления значений функции Дикмана с абсолютной погрешностью $\delta/(c_0 \cdot n)$, требует $O(n \ln^2 n)$ сложений и умножений и $O(n \ln n)$ делений с плавающей точкой. Коэффициенты $c_{k,i}$ не зависят от аргументов функций G_l , эти коэффициенты могут быть вычислены лишь один раз и сохранены в памяти машины. Поэтому трудоемкость их вычисления в общей оценке трудоемкости не учитывается.

Интегралы типа J зависят от параметров u, v, w, w_1, w_2 , а также от коэффициентов линейных функций l_1, l_2 и L , фигурирующих в формулах (20) и (21). Из описания предложенных методов следует, что параметры u, v и w этих интегралов могут пробегать лишь $O(n)$ возможных значений, а параметры $u - w, v - w, w_1, w_2$ и коэффициенты

линейных функций могут пробегать лишь $O(1)$ возможных значений. Каждый из рассматриваемых параметров и коэффициентов вычисляется с трудоемкостью $O(1)$ арифметических операций, поэтому вклад вычисления всех этих значений в общую оценку трудоемкости вычисления величин (30) составляет $O(n \ln n)$ арифметических операций.

Вычисление всех $O(n \ln n)$ интегралов (17), получаемых в ходе вычисления значений (12), требует $O(n \ln n)$ операций сложения и умножения с плавающей точкой, $O(n)$ операций деления (необходимых для обращения чисел вида $w - w_1$) и $O(1)$ операций вычисления логарифма (требуемых в тех случаях, когда $|w - w_1| \leq 1$). Обозначим эту трудоемкость через $T_{1,1}$.

Интегралы (18) вычисляются через интегралы вида

$$J_{2,2}^{(i)}(u, v, w, w_2) = \int_u^v (t - w)^i \cdot \ln(t - w_2) dt, \quad (31)$$

согласно методу, предложенному в [3]. Трудоемкость $T_{2,2}$ вычисления интегралов (31) является величиной $O(T_{1,1} + n \cdot T_0)$, где T_0 – трудоемкость вычисления одного логарифма. Трудоемкость $T_{2,1}$ вычисления интегралов (18) отличается от трудоемкости $T_{2,2}$ лишь константой в знаке O .

Интегралы (19) вычисляются через интегралы вида

$$\bar{J}_{2,2}^{(i)}(u, v, w, w_2) = \int_u^v (t - w)^i \cdot \ln(w_2 - t) dt \quad (32)$$

согласно методу, полностью аналогичному указанному выше, и оценка трудоемкости вычисления всех этих интегралов с точностью до константы совпадает с трудоемкостью $T_{2,2}$.

Как следует из раздела 3.1, интегралы (20) и (21) вычисляются через интегралы видов (18) и (19). Кроме того, для их вычисления требуется вычислить $O(n)$ интегралов вида (24), что сводится к $O(n \ln n)$ операциям сложения и умножения с плавающей точкой, $O(n)$ операциям деления и $O(n)$ операциям вычисления логарифма. Интегралы (18) и (19), как мы уже видели, в свою очередь вычисляются через интегралы (31) и (32). Таким образом, трудоемкость T_3 вычисления интегралов (20) и (21) имеет вид $T_3 = O(T_{1,1} + n \cdot T_0)$. Следует заметить, что хотя в приведенных методах всегда суммировалось константное количество членов геометрических прогрессий (исходя из соображений практической эффективности), однако для теоретически строгого контроля абсолютной погрешности с произвольным фиксированным количеством разрядов мантииссы, как показано выше, следует суммировать $O(\ln n)$ членов этих рядов.

Подводя итог, получаем, что трудоемкость вычисления значений (30) с фиксированной абсолютной погрешностью равна $O(n \ln n)$ операциям сложения и умножения с плавающей точкой, $O(n)$ операциям деления и $O(n)$ операциям вычисления логарифма.

5. Результаты вычислительных экспериментов

Существуют известные универсальные методы вычисления кратных интегралов. Для экспериментов и последующего сравнительного анализа нами были реализованы: метод Монте-Карло [1], метод Симпсона [1], метод Коробова [2], использующий параллелепипедальные сетки специального вида, а также методы, приведенные выше. Все программные коды написаны на языке С.

При сравнении методов нас интересуют две естественные характеристики: скорость и точность вычисления многомерных интегралов с помощью каждого из методов. Заметим, что точность методов, основанных на квадратурных формулах (это методы Монте-Карло, Симпсона и Коробова), надо задавать отдельно, и чем больше задаваемая точность, тем больше трудоемкость подсчета интеграла. Что же касается специализированных методов, предложенных в настоящей работе, то, как видно из их описания, отдельный параметр точности для них не требуется. Эффект ошибок округления незначителен и интегралы вычисляются с точностью чуть ниже максимальной, задаваемой разрядностью базового вещественного типа (для большинства приложений это тип `double` с 15 десятичных знаков мантиссы).

Как следует из теоремы 1 работы [4], естественно рассмотреть два случая: (i) $\alpha_2 > \beta_1$ и (ii) $\alpha_2 \leq \beta_1$, поскольку они приводят к существенно разным формулам для функций G_l , $l = 2, 3$. Во втором случае внутренние интегралы имеют нижнюю границу интегрирования λ_1 , являющуюся переменной интегрирования внешнего интеграла. Это показывает, что для использования квадратурных формул подынтегральную функцию надо умножить на характеристическую функцию отрезка $[\lambda_1; \beta_2]$. Наличие разрыва характеристической функции в точке λ_1 существенно увеличивает время вычисления интегралов с требуемой точностью.

Рассмотрим для начала случай (i). Зададим значения

$$\beta_0 = 0.05, \quad \alpha_1 = 0.10, \quad \beta_1 = 0.15, \quad \alpha_2 = 0.25, \quad \beta_2 = 0.35,$$

и посчитаем значения интегралов G_l при $l = 2, 3$ с точностью до 3, 4, 5 и 6 знаков мантиссы перечисленными универсальными методами.

В табл. 1 приведены получившиеся значения времени вычислений в секундах. Все вычисления проводились на персональном компьютере HP Z800 Workstation с двумя четырехядерными процессорами Intel Xeon E5540 2.53 GHz под операционной системой Windows 8 (использовалось лишь 1 ядро вычислителя). В последнем столбце таблицы приведены времена вычислений (с точностью не ниже 10^{-11}) специализированными методами, описанными в предыдущих разделах.

Таблица 1. Времена вычисления значений функций G_l , $l = 2, 3$

	Монте-Карло e-3...e-6	Симпсон e-3...e-6	Коробов e-3...e-6	Спецалгоритм
G_2	e-3: 6.80e-3	e-3: 1.90e-4	e-3: 1.79e-5	1.63e-5
	e-4: 6.12e-2	e-4: 1.90e-4	e-4: 3.06e-5	
	e-5: 6.30e-1	e-5: 7.24e-4	e-5: 8.36e-5	
	e-6: 1.96e+1	e-6: 2.81e-3	e-6: 2.23e-4	
G_3	e-3: 1.06e-1	e-3: 7.86e-3	e-3: 1.65e-4	3.43e-4
	e-4: 1.22e+0	e-4: 7.88e-3	e-4: 5.65e-4	
	e-5: 5.74e+0	e-5: 5.85e-2	e-5: 1.04e-3	
	e-6: 3.68e+2	e-6: 4.52e-1	e-6: 1.90e-3	

Из табл. 1 видно, что специализированные методы во всех случаях, кроме одного, являются наиболее быстрыми. Только для функции G_3 и точности 3 десятичных знака мантииссы метод квадратур Коробова работает быстрее специализированного алгоритма.

Теперь рассмотрим случай (ii). Зададим значения

$$\beta_0 = 0.05, \quad \alpha_1 = 0.10, \quad \beta_1 = 0.20, \quad \alpha_2 = 0.15, \quad \beta_2 = 0.35,$$

и посчитаем значения интегралов G_l при $l = 2, 3$ с точностью до 3, 4, 5 и 6 знаков мантииссы перечисленными универсальными методами. В табл. 2 приведены получившиеся значения времени вычислений в секундах. В последнем столбце приведены времена вычислений (с точностью не ниже 10^{-11}) специализированными методами, описанными в предыдущих разделах.

Таблица 2. Времена вычисления значений функций G_l , $l = 2, 3$

	Монте-Карло e-3...e-6	Симпсон e-3...e-6	Коробов e-3...e-6	Спецалгоритм
G_2	e-3: 3.36e-2	e-3: 1.44e-3	e-3: 4.58e-5	3.74e-5
	e-4: 3.06e-1	e-4: 1.42e-3	e-4: 9.34e-5	
	e-5: 1.44e+0	e-5: 5.52e-3	e-5: 2.52e-4	
	e-6: 7.20e+1	e-6: 2.17e-2	e-6: 4.57e-4	
G_3	e-3: 7.88e-1	e-3: 1.51e-2	e-3: 4.27e-4	1.51e-3
	e-4: 6.37e+0	e-4: 1.12e-1	e-4: 1.79e-3	
	e-5: 8.51e+1	e-5: 8.61e-1	e-5: 3.58e-3	
	e-6: 3.55e+2	e-6: 1.50e+3	e-6: 2.22e-1	

Таблица 2 позволяет сделать в точности тот же качественный вывод, что и табл. 1. Специализированные методы во всех случаях, кроме одного, являются наиболее быстрыми. Только для функции G_3 и точности 3 десятичных знака мантиссы метод квадратур Коробова работает быстрее специализированного алгоритма. Видимо, это связано с тем, что согласно доказанной выше теореме 1 вычисление значений функций G_3 сводится к вычислению 90 интегралов типа I_3 . Каждый такой интеграл является двукратным и вычисляется относительно сложным (по сравнению с однократным интегралом I_2) образом посредством метода, изложенного в разделе 3. Накопительный эффект больших констант и усложнений приводит к тому, что в итоге метод Коробова с 3 десятичными знаками оказывается в 2-3 раза быстрее.

Так как в предложенных методах многократно, а именно $\nu = O(n)$ раз совершенно независимо вычисляются значения интегралов видов F_2 и F_3 (см. формулы (12) и (22)) для различных наборов параметров в формулах, определяющих эти интегралы, то предложенные в работе методы допускают очевидное ν -кратное распараллеливание.

Список литературы

- [1] Бахвалов Н.С., *Численные методы. I*, М.: Наука, 1973, 631 с.
- [2] Коробов Н.М., *Теоретико-числовые методы в приближенном анализе*, М.: Изд. МЦНМО, 2004, 285 с.
- [3] Рыбаков А.С., “Модификация алгоритма оценки количества целых чисел интервала, имеющих не более трех больших простых делителей”, *Математические вопросы криптографии*, 4:3 (2013), 131–158.
- [4] Рыбаков А.С., “Оценки количества чисел со специальным разложением на простые множители”, *Математические вопросы криптографии*, 7:1 (2016), 119–142.
- [5] Aoki K., Bos J.W., Franke J., Gaudry P., Kleinjung T., Kruppa A., Lenstra A.K., Montgomery P.L., Osvisk D.A., te Riele H., Thome E., Timofeev A,

- Zimmermann P., “Factorization of a 768-bit RSA modulus”, web page, 2010, <http://www.loria.fr/~zimmerma/records/rsa768>.
- [6] Bach E., Peralta R., “Asymptotic semismoothness probabilities”, *Math. Comput.*, **65** (1996), 1701–1715.
- [7] Ekkelkamp W.H., *On the amount of sieving in factorization methods*, Ph.D. Thesis, Univ. Leiden, 2010, 106 pp.
- [8] Knuth D.E., Pardo L.T., “Analysis of a simple factorization algorithm”, *Theor. Comput. Sci.*, **3** (1976), 321–348.
- [9] Lambert R., *Computational aspects of discrete logarithms*, Ph.D. Thesis, Univ. Waterloo, 1996, 113 pp.
- [10] Lenstra A.K., Lenstra H.W., Jr., “The development of the number field sieve”, *Lect. Notes Math.*, **1554**, 1993, 131 pp.