тем обмена данными, использующих принципы радиоинтерфейса. Свободный выбор диапазона изменения целочисленных ИМР позволяет конструктору приемника эффективно решать задачу сложности реализации мягкого декодера.

Важное практическое значение имеет открывающаяся возможность адаптивного изменения интервала стирания путем смены параметра ρ для выработки ИМР в условиях изменения уровня сигнала. При этом поток оценок λ_i на некотором зачетном отрезке данных может явиться индикатором для смены выбранных параметров.

В случае исправления декодером помехоустойчивого кода стертых позиций решается вопрос об идентификации ложных стираний и назначении приоритетов при перестановочном декодировании или декодировании на основе эквивалентных кодов.

Внедрение широкополосных систем обмена данными, применение в них сложных видов модуляции и недвоичных кодовых конструкций открывает новые возможности для мягкого декодирования таких кодов и решения важной задачи снижения сложности реализации декодеров недвоичных кодов

Литература

1. Скляр Б. Цифровая связь. М.: Радио и связь, 2000. – 800 с.
2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005. – 320 с.
3. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. Ульяновск: Изд. УлГТУ, 2010. – 379 с.
4. Волков Л.Н., Немировский М.С., Шинаков Ю.С. Системы цифровой радиосвязи: базовые методы и характеристики. М.: Эко-Трендз, 2005. – 392 с.
5. Возенкрафт Дж., Джекобс И. Теоретические основы техники связи. М.: Мир, 1969. – 640 с.
6. Тихонов В.И., Харисов В.Н. Статистический анализ и синтез радиотехнических устройств и систем. М.: Радио и связь, 1991. – 410 с.
7. Шувалов В.П. Прием сигналов с оценкой их качества. М.: Связь. 1979. – 240 с.
8. Гладких А.А., Мансуров А.И, Черторийский С.Ю. Статистическая оценка индексов достоверности символов, формируемых в системе с мягким декодированием // ИКТ. Т.6, №1, 2008. – С. 39-43.

NUMERICAL SIMULATION OF THE GENERALIZED PROCEDURE OF FORMATION OF INDICES OF SOFT DECISIONS

Gladkikh A.A., Klimov R.V.

Offers a universal method for calculating indices of soft decisions necessary for the effective implementation of the procedure of soft decoding error-correcting codes. Introduce efficiency index scheme for forming indices soft decision and its asymptotic limits for different types of signals. Boundary estimates an analytical modeling synthesized systems forming indices of soft decisions are verified by results of statistical tests appropriate models.

Keywords: *indices of soft decisions, numerical simulation.*

Гладких Анатолий Афанасьевич, к.т.н., профессор Кафедры телекоммуникаций Ульяновского государственного технического университета (УлГТУ). Тел. (8-842) 277-80-82. E-mail: a.gladkikh@ulstu.ru

Климов Роман Владимирович, студент УлГТУ. Тел. 8-917-631-32-57. E-mail: chorrus@mail.ru

УДК 519.6

УСКОРЕННЫЙ МЕТОД ВЫЧИСЛЕНИЯ ЗНАЧЕНИЙ ЛОГАРИФМИЧЕСКОЙ ФУНКЦИИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ФОРМИРОВАНИЯ СИСТЕМ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Жук А.П., Орел Д.В.

В работе предложен ускоренный численный метод вычисления значений логарифмической функции для решения задачи формирования систем квазиортогональных кодовых последовательностей на основе функциональных преобразований ее псевдослучайных аргументов, который позволяет снизить необходимое количество арифметических операций.

Ключевые слова: численный метод, системы кодовых последовательностей, функциональное преобра-

зование, псевдослучайный аргумент, логарифмическая функция, число операций

Последние годы возрастает актуальность обеспечения защищенности информационного обмена в спутниковых радионавигационных системах (СРНС) между навигационными космическими аппаратами (НКА) и аппаратурой потребителей (АП). В качестве варианта решения указанной задачи в работе [2] приведена методика повышения структурной скрытности НС СРНС на основе стохастического использования различных уникальных систем квазиортогональных кодовых последовательностей с требуемыми характеристиками. В работе [3] предложен вариант получения необходимого количества систем квазиортогональных кодовых последовательностей на основе метода функциональных преобразований псевдослучайных аргументов. Реализация предложенного метода на практике включает в себя следующие основные этапы.

1. Формирование исходного ряда равномерно распределенных псевдослучайных чисел rnd.

2. Функциональное преобразование псевдослучайных чисел с помощью выбранной функции $\tau_i = G^{-1}(rnd_i)$.

3. Дискретизация полученных действительных значений функции τ_i с выбранным шагом d для получения натуральных значений длин серий элементов в формируемых двоичных кодовых последовательностях: $t_i = \left]\tau_i / d\right[$.

4. Получение двоичной последовательности, в которой t_i определяет длину серии последовательно идущих элементов одного знака: $n_{t_{i-1}+1} \ldots n_{t_{i-1}+t_i} = (-1)^i \ (a_{t_{i-1}+1} \ldots a_{t_{i-1}+t_i})$, где $a_1 \ldots a_N$ – последовательность единичных элементов.

На рис. 1 наглядно проиллюстрирована суть предложенного метода. Как было отмечено в [4], кодовые последовательности обладают оптимальными корреляционными характеристиками в том случае, когда серии элементов в них подчиняются закону k-распределенности. Такое распределение серий элементов достигается в полной мере при использовании функции вида

$$\tau = \log_2 \frac{1}{rnd}.$$

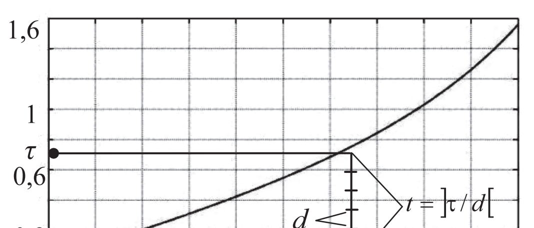

Рис. 1. Иллюстрация метода функциональных преобразований псевдослучайных аргументов

При достаточно большом периоде генератора псевдослучайных чисел (ГПСЧ) можно получить большое число неповторяющихся кодовых последовательностей: при длине периода ГПСЧ равному N количество кодовых последовательностей, которое теоретически может быть получено при использовании единственного функционального преобразования, составит $Q \approx 2N/l$, где l – длина кодовых последовательностей в битах. Поскольку расчетное время эксплуатация НКА не превышает 15 лет, достаточно обеспечить защищенность НС на указанный период. Необходимое количество кодовых последовательностей для обеспечения защищенности НС в течение 15 лет составляет $A_r = 2{,}3652 \cdot 10^{12}$ [3]. При этом должно выполняться следующее неравенство: $Q \geq A_r$. Тогда при длине последовательностей $l = 10230$ бит $N \geq 1{,}2098 \cdot 10^{16}$.

ГПСЧ «Вихрь Мерсенна» имеет период $N = (2^{19937} - 1)/32 \approx 1{,}3486 \cdot 10^{6000}$, который многократно превосходит значение A_r и удовлетворяет приведенному неравенству. Поскольку вышесказанное доказывает, что при использовании ГПСЧ «Вихрь Мерсенна» можно с помощью лишь одной функции получить необходимое количество последовательностей для защиты НС в течение 15 лет, то целесообразно использовать единственную функцию $\tau = \log_2 \frac{1}{rnd}$, поскольку она обеспечивает k-распределенность серий элементов в получаемых кодовых последовательностях. При этом выбор начального бита ГПСЧ в качестве секрета позволит обеспечить высокую структурную скрытность кодовых последовательностей.

Метод получения систем двоичных квазиортогональных кодовых последовательностей на основе функциональных преобразований псевдослучайных аргументов предполагает вычисление значений функции с определенной точностью. Согласно стандарту IEEE 754-2008 [5] в подавляющем большинстве современных устройств числовые данные обрабатываются в формате представления чисел с плавающей точкой и имеют определенный класс точности: половинную, одинарную, двойную или расширенную. Особенности представления чисел с различной точностью представлены в таблице 1 (S – знак, E – показатель степени, I – целая часть, F – дробная часть).

Таблица 1. Особенности представления чисел с различной точностью

Точность / Характеристики	Половинная (half-precision)	Одинарная (single-precision)	Двойная (double-precision)	Двойная расширенная (double-extended precision)
Размер слова (байты)	2	4	8	10
Число десятичных знаков	3	7	15	19
Наименьшее значение	$5{,}96\cdot10^{-8}$	$1{,}2\cdot10^{-38}$	$2{,}3\cdot10^{-308}$	$3{,}4\cdot10^{-4932}$
Наибольшее значение	65504	$3{,}4\cdot10^{38}$	$1{,}7\cdot10^{308}$	$1{,}1\cdot10^{4932}$
Поля	S-E-F	S-E-F	S-E-F	S-E-I-F
Размеры полей, бит	1-5-10	1-8-23	1-11-52	1-15-1-63

Поскольку частота трансляции некоторых НС достигает 10,23 МГц, каждую секунду требуется формирование до 10 230 000 бит дальномерного кода. Для формирования двоичных последовательностей на основе предложенного метода с такой скоростью с использованием стандартных классов точности представления чисел требуется выполнять порядка 10^4-10^8 операций в сек. В то же время известно [6], что бортовые ЭВМ НКА способны осуществлять до $2{,}1\cdot10^6$ операций в сек. Таким образом, в некоторых случаях всех имеющихся вычислительных ресурсов бортовой ЭВМ будет недостаточно для формирования кодовых последовательностей. Повышение производительности бортовой ЭВМ ограничивается допустимыми массогабаритными параметрами и максимальным возможным энергопотреблением. Учитывая, что бортовая ЭВМ НКА должна выполнять и другие задачи, помимо вычисления значений функции, актуальность приобретает задача снижения требуемых вычислительных ресурсов для вычисления значений функции до нижней границы диапазона - 10^4 операций в секунду.

Целью статьи является снижение максимального необходимого числа операций при нахождении значений логарифмической функции для получения возможности реализации в СРНС метода формирования увеличенного количества систем квазиортогональных кодовых последовательностей на основе функциональных преобразований псевдослучайных аргументов.

Известно, что чаще всего вычисления производятся с двойной точностью [8], которая обеспечивает относительную точность в 15 десятичных символов. Так, например, функциональное преобразование $\tau=\log_2\frac{1}{rnd}$ при $rnd=0{,}21$ с двойной точностью составляет $\tau=2{,}25153876\,6995965$. В то же время в методе [3] получения систем квазиортогональных кодовых последовательностей результат функционального преобразования τ при шаге дискретизации $d=1$ округляется в большую сторону до ближайшего целого. Найденное значение будет преобразовано следующим образом: $\tau=2{,}25153876\,6995965\rightarrow t=3$.

Тогда вычисление τ допустимо производить с меньшей точностью, отбрасывая всю дробную часть числа и увеличивая на единицу его целую часть.

Как известно, в цифровой электронной вычислительной технике для вычисления значений различных функций применяются различные численные методы [9]. Численные методы позволяют вычислять приближенные значения функций: численным методом обычно решается некоторая другая, более простая задача, аппроксимирующая (приближающая) исходную задачу. В ряде случаев используемый численный метод строится на базе бесконечного процесса, который в пределе приводит к искомому решению. Примером этого может служить вычисление значений элементарной функции с помощью частичных сумм степенного ряда, в который разлагается эта функция. Однако реально предельный переход обычно не удается осуществить, и процесс, прерванный на некотором шаге, дает приближенное решение. Таким образом, осуществляется аппроксимация функции, позволяющая вычислить ее значение с необходимой точностью. Точность вычисления значения функции, как известно, определяется количеством слагаемых при разложении функции в ряд.

Для приближения функций, у которых достаточно просто вычисляются старшие производные, широко используется ряд Тейлора. К таким функциям относится и натуральный логарифм. Ряд Тейлора для функции натурального логарифма имеет вид:

$$\ln(1+x)=\frac{x}{1!}-\frac{1x^2}{2!}+\frac{2x^3}{3!}-\frac{6x^3}{4!}\cdots+$$
$$+\frac{(-1)^{n+1}(n-1)!x^n}{n!}=\frac{x}{1!}-\frac{1!x^2}{2!}+\frac{2!x^3}{3!}-\frac{3!x^3}{4!}\cdots+$$
$$+\frac{(-1)^{n+1}(n-1)!x^n}{n!}=x-\frac{x^2}{2}+\frac{x^3}{3}-\cdots+$$
$$+\frac{(-1)^{n+1}x^n}{n}=\sum_{n=0}^{\infty}\frac{(-1)^n x^{n+1}}{n+1}=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}x^n}{n}, \quad (1)$$

для всех $x\in(-1{,}1]$.

Если аргументом *x* функции и соответствующего ей функционального ряда является действительное число, то аргумент *x* и в функции, и в числовом ряде можно заменить произвольной функцией $Q'(x)$ при единственном условии, что функция во всей области определения выражается действительным числом. Это положение основывается на принципе суперпозиции, а такой метод образования новых функций и их разложений в ряд называется композиционным [10].

Ограничение значения переменной $x \in (-1,1]$ можно записать иначе следующим образом: $-1 < x \le 1$. Тогда составной аргумент функции натурального логарифма должен находиться в интервале $0 < 1 + x \le 2$. Поскольку значения аргумента rnd принимают значения $0 < rnd < 1$, то область возможных значений rnd при замене аргумента функции полностью входит в область допустимых значений аргумента функции натурального логарифма $(1 + x)$.

Используя формулы преобразований логарифмов, получим следующее:

$$\tau = \log_2 \frac{1}{rnd} = \frac{\ln \frac{1}{rnd}}{\ln 2} = \frac{\ln(rnd^{-1})}{\ln 2} = \\ = \frac{-\ln rnd}{\ln 2} = -\frac{1}{\ln 2} \ln rnd. \tag{2}$$

Произведем замену аргумента $rnd = 1 + x$. Выразим x: $x = rnd - 1$. Тогда выражение (2) будет выглядеть следующим образом:

$$\tau = -\frac{1}{\ln 2} \ln rnd = -\frac{1}{\ln 2} \ln(1+x) = \\ = -\frac{1}{\ln 2} \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^n}{n} = \\ = -\frac{1}{\ln 2} \sum_{n=1}^{\infty} \frac{(-1)^{n+1} (rnd-1)^n}{n} = \\ = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}(1-rnd)^n}{n \ln 2}. \tag{3}$$

Разложение логарифмической функции $\tau = \log_2 \frac{1}{rnd}$ в ряд Тейлора имеет вид

$$\tau = \log_2 \frac{1}{rnd} = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}(1-rnd)^n}{n \ln 2}. \tag{4}$$

При этом количество слагаемых ряда n определяется в зависимости от необходимой точности вычисления значения функции. Чем большая точность требуется, тем большее количество слагаемых ряда необходимо для вычисления значения функции.

Согласно второму следствию из теоремы Лейбница остаток сходящегося знакочередующегося ряда $R_n = S - S_n$, где $S = \sum_{i=1}^{\infty} b_i$, $S_n = \sum_{i=1}^{n} b_i$, будет по модулю меньше первого отброшенного слагаемого: $|R_n| < |b_{n+1}|$. В свою очередь для нахождения суммы числового ряда с определенной точностью ε первое отбрасываемое слагаемое b_{n+1} должно быть по модулю меньше значения ε: $|\varepsilon| > |b_{n+1}|$. Это позволяет сделать заключение о том, что нахождение неполной суммы слагаемых числового ряда $S_n = \sum_{i=1}^{n} b_i$ без учета всех последующих слагаемых начиная с b_{n+1} позволит вычислить значение функции с точностью ε.

Поскольку первое отброшенное слагаемое равно

$$b_{n+1} = \frac{(-1)^{n+1}(1-rnd)^{n+1}}{(n+1) \cdot \ln 2}, \tag{5}$$

то для оценки минимального необходимого количества слагаемых необходимо решить следующее неравенство:

$$|\varepsilon| > \left| \frac{(-1)^{n+1}(1-rnd)^{n+1}}{(n+1) \cdot \ln 2} \right|, \tag{6}$$

то есть найти такое наибольшее n относительно минимального и максимального значений аргумента rnd, при котором неравенство (6) верно.

Поскольку в неравенстве (6) значения обеих частей приведены по модулю, а значение точности всегда будет выражаться положительным числом, то знак последнего отбрасываемого члена можно не учитывать. Тогда:

$$\varepsilon > \frac{(1-rnd)^{n+1}}{(n+1) \ln 2}. \tag{7}$$

Поскольку $\ln 2$ – число, перенесем его в левую часть неравенства:

$$\varepsilon \ln 2 > \frac{(1-rnd)^{n+1}}{n+1}.$$

Как было упомянуто в [7], скорость сходимости ряда $Q(x) = \ln(1+x)$ меняется на его круге сходимости: при значениях *x* из центра круга сходимости ряд сходится быстро, в то время как при значениях *x*, близких к границам круга сходимости, ряд сходится медленнее. Для определения минимального необходимого числа слагаемых числового ряда необходимо решить неравенство (8) относительно *n*. Поскольку неизвестно способов выражения *n* из неравенства (8), решить его возможно аналитическим или графическим путем.

Учитывая, что граничные значения не включаются в промежуток (0;1), а минимальная разница между соседними псевдослучайными числами составляет 10^{-4} для формирования кодовых последовательностей длиной 10230 бит, то минимальное и максимальное значения аргумента будут соответственно равны $rnd_{\min} = 10^{-4}$ и $rnd_{\max} = 0{,}9999$.

Почленное вычитание логарифмических рядов позволяет переходить к другим видам функций и их разложений. Существует альтернативный способ представления аргумента логарифмической функции, при использовании которого, как отмечается в [11], минимально необходимое количество слагаемых для нахождения значения функции с заданной точностью при минимальном значении аргумента существенно меньше, чем при рассмотренном выше способе. С учетом свойства логарифмической функции

$$\ln\frac{1+x}{1-x} = \ln(1+x) - \ln(1-x), \qquad (9)$$

функция $\ln(1-x)$ может быть разложена в ряд Тейлора следующим образом:

$$\ln(1-x) = -x - \frac{x^2}{2!} - \frac{2x^3}{3!} - \frac{6x^4}{4!} - \cdots - \frac{(n-1)!\,x^n}{n!} =$$
$$= -x - \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^4}{4} - \cdots - \frac{x^n}{n}.$$

В свою очередь, функция $\ln(1+x)$ раскладывается в ряд Тейлора согласно выражению (1). Тогда разложение функции $\ln\frac{1+x}{1-x}$ в ряд Тейлора примет вид:

$$\ln\frac{1+x}{1-x} =$$
$$= x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots + x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} - \cdots =$$
$$= 2\left(x + \frac{x^3}{3} + \frac{x^5}{5} + \frac{x^7}{7} + \cdots\right),$$

$$\ln\frac{1+x}{1-x} = 2\sum_{n=1}^{\infty}\frac{x^n}{n},\ n = 1;3;5;7\ \ldots \qquad (10)$$

Представленный числовой ряд (10) имеет круг сходимости при $x \in (-1;1)$, тогда аргумент функции лежит в пределах $0 < \frac{1+x}{1-x} < \infty$. В свою очередь, в этот диапазон полностью входит область допустимых значений аргумента функции

$$\tau = \log_2\frac{1}{rnd}:\ 0 < rnd < 1 .$$

Числовой ряд на основе функции $\ln\frac{1+x}{1-x}$, так же как и ряд на основе функции $\ln(1+x)$, будет иметь различную скорость сходимости на различных участках круга сходимости. Исследования [10] показывают, что в некоторых случаях использование такого разложения в ряд существенно сокращает количество слагаемых числового ряда, сумму которых необходимо найти для вычисления значения функции.

Произведем замену аргумента: $rnd = \frac{1+x}{1-x}$. Тогда

$$\tau = -\frac{1}{\ln 2}\ \ln rnd = -\frac{1}{\ln 2}\ \ln\frac{1+x}{1-x} =$$
$$= -\frac{1}{\ln 2}\ 2\sum_{n=1}^{\infty}\frac{x^n}{n} = -\frac{2}{\ln 2}\sum_{n=1}^{\infty}\frac{x^n}{n}. \qquad (11)$$

Неравенство $|\varepsilon| > |b_{n+1}|$ будет выглядеть следующим образом:

$$|\varepsilon| > \left|-\frac{2}{\ln 2}\ \frac{x^{n+1}}{n+1}\right|. \qquad (12)$$

Значения x при различных rnd представлены в таблице 2.

Таблица 2. Значения x при различных значениях rnd .

rnd	0,9999	0,5	0,0001
x	$-\frac{9999}{10001}$ $-0{,}9998$	$-\frac{1}{3}$ $-0{,}3333$	$-\frac{1}{19999}$ $-0{,}00005$

Поскольку обе части неравенства рассматриваются по модулю, то знак «–» в правой его части не влияет на результат, его можно опустить. По этой же причине можно опустить и знак аргумента x, поэтому допустимо использовать модуль x.

В таблице 3 представлены результаты исследований числа слагаемых числового ряда, сумму которых необходимо найти для вычисления значения функции с обозначенной точностью.

Как видно из таблицы 3, при первом способе представления аргумента в виде $rnd = 1+x$ максимальное число слагаемых требуется для нахождения значения функции при наименьшем возможном значении аргумента. Наоборот, при втором рассмотренном способе представления аргумента в виде $rnd = \frac{1+x}{1-x}$ максимальное число слагаемых числового ряда требуется при нахождении значения функции при максимальном значении аргумента.

Таблица 3. Число слагаемых числового ряда для вычисления значения логарифмической функции с различной точностью

Точ-ность	Тип замены аргумента	Значение аргумента rnd		
		10^{-4}	0,5	0,9999
10^{-15}	$rnd = 1 + x$	225 768	44	3
	$rnd = \frac{1+x}{1-x}$	3	29	119 523
10^{-3}	$rnd = 1 + x$	1 270	7	1
	$rnd = \frac{1+x}{1-x}$	1	5	1 953
1	$rnd = 1 + x$	1	1	1
	$rnd = \frac{1+x}{1-x}$	1	1	1

При уменьшении точности уменьшается и число слагаемых числового ряда для вычисления функции. Использование второго способа разложения функции в ряд с представлением аргумента в виде $rnd = \frac{1+x}{1-x}$ в большинстве случаев позволяет сократить минимальное необходимое число слагаемых для вычисления значения функции по сравнению с первым способом разложения функции в ряд при представлении аргумента в виде $rnd = 1 + x$. Для вычисления значения функции с точностью до единицы требуется найти всего одно слагаемое числового ряда при любом представлении аргумента.

Таким образом, при практической реализации метода формирования систем квазиортогональных кодовых последовательностей на основе преобразования $\tau = \log_2 \frac{1}{rnd}$ требуется найти первое слагаемое числового ряда Тейлора, которое является первой производной функции τ. На основе выражения:

$$\tau = \log_2 \frac{1}{rnd} = \frac{1}{\ln 2} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}(1-rnd)^n}{n} \qquad (13)$$

первое слагаемое ряда Тейлора будет иметь следующий вид:

$$\tau^{(1)} = \frac{1-rnd}{\ln 2}. \qquad (14)$$

Тогда вычисление значения функции с точностью до целого значения можно представить в следующем виде:

$$\tau = \log_2 \frac{1}{rnd} = \left[\frac{1-rnd}{\ln 2}\right]. \qquad (15)$$

Уменьшение минимального необходимого числа слагаемых числового ряда для вычисления значения функции приведет к снижению количества выполняемых арифметических операций и увеличению скорости вычисления этого значения. Выражение (15) представляет собой ускоренный метод вычисления значений функции $\tau = \log_2 \frac{1}{rnd}$. Вычисление логарифма в (15) заменено на элементарные операции вычитания, деления и округления до целого, поэтому оно может быть положено в основу работы блока вычисления значения функционального преобразования.

Оценим повышение скорости вычисления ΔV значения функции с точностью до единицы относительно скорости вычисления значения функции с половинной точностью при формировании одной кодовой последовательности длиной 10230 бит. Для этого необходимо вычислить разность между числом арифметических операций, необходимых для вычисления значений функции при обоих классах точности при одном и том же значении аргумента: $\Delta K_i = K_{n_i} - K_{ed_i}$, где $\Delta K_i = K_{n_i} - K_{ed_i}$ – разность между числом слагаемых числового ряда, необходимых для вычисления значения функции с половинной точностью (K_{n_i}) и с точностью до единицы (K_{ed_i}) при одинаковом значении аргумента. Необходимо вычислить такие разности для требуемого количества аргументов. Найдем повышение скорости вычисления с точностью до первого знака после запятой, в таком случае будет достаточно найти разности для 33 значений аргумента, равномерно распределенных по области определения: $i = 33$. Тогда повышение скорости вычисления можно найти как среднее арифметическое между найденными разностями ΔK_i на основе следующей формулы:

$$\Delta V = \frac{\sum_{i=1}^{n} \Delta K_i}{i}. \qquad (16)$$

Поскольку график зависимости числа слагаемых числового ряда от значения аргумента Θ при использовании класса половинной точности $\varepsilon = 10^{-3}$ является нелинейным, то необходимо осуществить аппроксимацию зависимости Θ методом наименьших квадратов [9]. В таблице 4 приведены 33 опорные точки, представляющие собой число слагаемых числового ряда для вычисления значения функции при равномерно распределенных значениях аргумента на области определения с точностями $\varepsilon = 10^{-3}$ и $\varepsilon = 10^{0} = 1$.

Таблица 4. Число слагаемых для вычисления значения логарифмической функции с различной точностью для 33 значений аргумента

Значение аргумента	Точность		Значение аргумента	Точность		Значение аргумента	Точность	
	10^{-3}	1		10^{-3}	1		10^{-3}	1
	Число слагаемых			Число слагаемых			Число слагаемых	
0,0001	1270	1	0,3437	11	1	0,6875	4	1
0,0312	88	1	0,375	11	1	0,7187	4	1
0,0625	52	1	0,4062	9	1	0,75	4	1
0,0937	37	1	0,4375	8	1	0,7812	3	1
0,125	29	1	0,4687	8	1	0,8125	3	1
0,1562	24	1	0,5	7	1	0,8437	3	1
0,1875	20	1	0,5312	7	1	0,875	3	1
0,2187	17	1	0,5625	6	1	0,9062	2	1
0,25	15	1	0,5937	6	1	0,9375	2	1
0,2812	14	1	0,625	5	1	0,9687	1	1
0,3125	12	1	0,6562	5	1	0,9999	1	1

Как видно из таблицы 4, при точности $\varepsilon = 10^{-3}$ число слагаемых ряда Тейлора постепенно уменьшается при увеличении значения аргумента. При точности $\varepsilon = 1$ число слагаемых ряда Тейлора, необходимое для вычисления значения функции, равно одному при любом значении аргумента. При одном слагаемом ряда Тейлора количество арифметических операций для формирования кодовой последовательности длиной 10230 элементов составляет порядка 10^4 операций в секунду.

На основе опорных точек из таблицы 4 методом наименьших квадратов с помощью полинома 20 степени была построена аппроксимирующая функция Θ для класса половинной точности, $\varepsilon = 10^{-3}$. Она представлена на рис. 3.

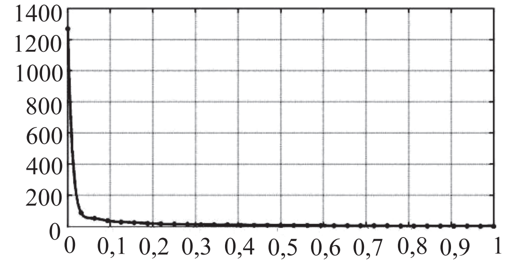

Рис. 3. Опорные точки, характеризующие число слагаемых ряда Тейлора для вычисления значения функции τ и аппроксимированная функция Θ для точности $\varepsilon = 10^{-3}$

Затем были выбраны 5263 точки, равномерно распределенные на интервале [0,0001;0,9999] с шагом 0,00019. Такое число аргументов близко к количеству серий элементов в кодовой последовательности длиной 10230 бит. Для выбранных аргументов были найдены значения K_{n_i} аппроксимирующей функции Θ. На основе найденных значений K_{n_i} по формуле (16) был вычислен коэффициент увеличения скорости вычислений значений функции с точностью до единицы относительно скорости вычисления значения функции с половинной точностью при формировании одной кодовой последовательности: $\Delta V = 23{,}95$. Некоторые данные, показывающие увеличение скорости вычислений значений функции, приведены в таблице 4. Так, например, при значении аргумента $rnd = 0{,}1562$ число арифметических операций при понижении точности вычисления сократилось в 24 раза, поскольку количество слагаемых числового ряда, необходимых для вычисления значения функции, сократилось с 24 до 1.

Выводы

1. При практической реализации метода получения систем квазиортогональных кодовых последовательностей на основе функциональных преобразований псевдослучайных аргументов необходимо производить вычисления значений функции $\tau = \log_2 \frac{1}{rnd}$, обеспечивающей *k*-распределенность серий элементов в последовательностях,

2. Нахождение значений логарифмической функции $\tau = \log_2 \frac{1}{rnd}$ при помощи численного метода разложения в ряд Тейлора при использовании стандартных классов точности представления двоичных чисел требуется выполнять порядка 10^4-10^8 операций в с, в то время как бортовые ЭВМ НКА способны осуществлять до $2{,}1 \cdot 10^6$ операций в с. В связи с этим возникает необходимость снижения требуемого для вычисления значений функции количества арифметических операций до нижней границы диапазона 10^4 операций в с.

3. В используемом методе получения систем квазиортогональных кодовых последовательностей на основе функциональных преобразований псевдослучайных аргументов значения функции используются как длины серий элементов и округляются до целых значений, поэтому точность вычисления значений функции может быть уменьшена.

4. Вычисление значения функции $\tau = \log_2 \frac{1}{rnd}$ с точностью до целого числа можно приблизить использованием всего одного слагаемого числового ряда Тейлора на всем интервале области определения функции и перейти к выражению,

в котором производятся элементарные операции вычитания, деления и округления вверх.

5. Предложенный ускоренный численный метод вычисления значений логарифмической функции $\tau = \log_2 \frac{1}{rnd}$ позволяет сократить минимальное необходимое число арифметических операций для вычисления значений функции. Скорость вычисления повышается более чем в 23 раза по сравнению с вычислением значений функции с половинной точностью, а количество арифметических операций достаточно порядка 10^4 операций в с.

Литература

1. Global Navigation Space Systems: reliance and vulnerabilities // Report of The Royal Academy of Engineering. London: March, 2011. – 48 p.
2. Жук А.П., Орел Д.В. Разработка методики повышения структурной скрытности сигналов спутниковых радионавигационных систем // Вестник СГУ. №5 (70), 2010. – С. 44-52.
3. Жук А.П., Фомин Л.А., Романько Д.В., Орел Д.В. Использование класса особых сигналов для передачи информации в радиосистемах с кодовым разделением каналов // Нейрокомпьютеры Разработка и применение. №1, 2010. – С. 40-45.
4. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. – 152 с.
5. IEEE Computer Society (August 29, 2008). IEEE Standard for Floating-Point Arithmetic, IEEE.
6. Eickhoff J. Onboard computers, onboard software and satellite operations. Springer, 2012. – 277 p.
7. Урличич Ю.М., Субботин В.А., Ступак Г.Г., Дворкин В.В., Поваляев А.А., Карутин С.Н. Инновация: ГЛОНАСС. Стратегия развития. // Спутниковая навигация и КВНО. Обзор по материалам СМИ. М.: ЦНИИмаш, №2, 2011. – С.18-23.
8. Monniaux D. The pitfalls of verifying floating-point computations. ACM Transactions on Programming Languages and Systems 30 (3): May 2008, Article #12.
9. Волков Е.А. Численные методы. М.: Наука, 1987. – 248 с.
10. Алексеева Е.Е. Разложение в степенной ряд логарифмических функций // Современные научные достижения. Математика. Белгород: Руснаучкнига, 2012. – 120 с.
11. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. Т.2. М.: ФИЗ-МАТЛИТ, 2001. – 810 с.

THE ACCELERATED METHOD OF CALCULATION LOGARITHMIC FUNCTION VALUES FOR THE TASK SOLUTION OF GENERATION CODE SETS

Zhuk A.I., Orel D.V.

In work is offered the accelerated numerical method of calculation logarithmic function values for the task solution of generation quasi-orthogonal code sets on the basis of functional transformations of pseudorandom arguments. This allows to reduce minimal necessary number of arithmetic operations.

Keywords: *numerical method, code sets, functional transformation, pseudorandom argument, logarithmic function, number of operations.*

Жук Александр Павлович, к.т.н., профессор Кафедры организации и технологии защиты информации (ОТЗИ) Северо-Кавказского федерального университета (СКФУ). Тел. (8-865) 235-74-09; 8-918-884-14-81. E-mail: alekszhuk@mail.ru

Орел Дмитрий Викторович, ассистент Кафедры ОТЗИ СКФУ. Тел. (8-865) 295-56-36; 8-918-740-11-74. E-mail: orel@otzi-ncfu.ru

УДК 621.391

КОНЦЕПЦИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ТЕЛЕФОНИИ

Галактионов К.И., Кузнецов М.В.

В статье рассмотрена концепция построения сетей голосовой связи на базе облачных технологий. В частности, описывается возможная методика их интеграции в сети следующего поколения. Рассматривается понятие облачной маршрутизации.

Ключевые слова: телефонные сети общего пользования, облачная маршрутизация, сети следующего поколения, Skype, VoIP, конвергенции услуг, сетевая инфраструктура.

Процесс конвергенции раздельно существующих сетей и систем в отдельных случаях способен продолжаться до полного их слияния. Примером этого могут служить базовые принципы органи-