Численный метод вычисления коэффициентов позиционной весомозначной системы счисления для выполнения обратного преобразования и коррекции ошибки в модулярном коде

И.А. Калмыков [1], А.А. Оленев [1], Т.А. Пелешенко [1], Н.К. Чистоусов[1], К.С. Фоменко [1]
[1] Федеральное государственное автономное образовательное учреждение высшего образования Северо-Кавказский федеральный университет, 355017, г. Ставрополь, ул. Пушкина, д.1

Аннотация

Одним из эффективных методов повышения производительности систем цифровой обработки сигналов является использование параллельных арифметических кодов, в частности, полиалфавитных полиномиальных модулярных кодов. В этих кодах для выполнения модульных операций (сложение, вычитание, умножение) требуются меньшие временные затраты по сравнению с выполнением этих операций в позиционных кодах. Это достигается за счет независимого выполнения этих операций по модулям кода. Однако такая организация вычислений требует перевода из позиционных кодов в полиалфавитные полиномиальные модулярные коды, а после вычислений – выполнения обратного перевода. Известно, что последняя операция требует достаточно больших временных и схемных затрат. Для устранения данной проблемы был разработан численный метод вычисления коэффициентов позиционной весомозначной системы счисления из кодовой комбинации полиалфавитного полиномиального модулярного кода, позволяющего эффективно выполнить обратное преобразование. Полученные с помощью этого метода коэффициенты можно также использовать для поиска и коррекции ошибок, возникающих в процессе вычислений при цифровой обработке сигналов. Использование изоморфизма Китайской теоремы об остатках позволило уменьшить временные и схемные затраты при вычислении коэффициентов позиционной весомозначной системы счисления из модулярного кода.

Ключевые слова: полиалфавитные полиномиальные модулярные коды, численные методы, коэффициенты позиционной весомозначной системы счисления, обратное преобразование, коррекция ошибок в модулярном коде.

Цитирование: **Калмыков**, **И.А.** Численный метод вычисления коэффициентов позиционной весомозначной системы счисления для выполнения обратного преобразования и коррекции ошибки в модулярном коде / И.А. Калмыков, А.А. Оленев, Т.А. Пелешенко, Н.К. Чистоусов, К.С. Фоменко // Компьютерная оптика. – 2026. – Т. 50, № 4. – 1857. – doi: 10.18287/COJ1857.

Citation: Kalmykov IA, Olenev AA, Peleshenko TA, Chistousov NK, Fomenko KS. A numerical method for calculating coefficients of a positional weight-valued number system for performing the inverse transform and error correction in a modular code. Computer Optics 2026; 50(4): 1857. doi: 10.18287/COJ1857.

Введение

Одной из наиболее перспективных областей применения модулярных кодов (МК), к которым относятся код системы остаточных классов (СОК) и арифметический полиалфавитный полиномиальный модулярный код (ППМК), является цифровая обработка сигналов (ЦОС). Это связано с тем, что в задачах ЦОС используются операции сложения, вычитания и умножения, а большинство из них должно выполняться в реальном масштабе времени (РМВ). Для обеспечения РМВ при обработке речи требуется выполнить 10^7 операций типа «умножение-сложение» (оп) в секунду при использовании 16-разрядных данных. Обработка изображений размером 1024×1024 точек с глубиной 32 бита в РМВ потребует выполнения до 10^9 оп/с. Фильтрация сигналов в радиолокации при обработке 214 отсчетов требует выполнения до 10^9 оп/с [1]. Поэтому для обеспечения РМВ при выполнении задач ЦОС в работах [2 – 6] было предложено использовать модулярные коды. В качестве элементной базы авторы выбирают технологии ASIC и FPGA, которые имеют низкую цену, малую потребляемую мощность и достаточно высокое быстродействие. К достоинствам МК можно отнести и их способность обнаруживать и корректировать ошибки вычислений [7 – 10]. Однако это негативно сказывается на схемных затратах и производительности систем ЦОС, так как процесс поиска и исправления ошибок выполняется независимо от обязательной процедуры обратного преобразования из МК в позиционный код (ПК). Таким образом, имеет место следующая проблема. С одной стороны, для обеспечения отказоустойчивости систем ЦОС в их состав вводят блоки обнаружения и коррекции ошибок, а, с другой стороны, это приводит к увеличению схемных и временных затрат на цифровую обработку сигналов. Постановка задачи исследования: для решения выявленной проблемы необходимо разработать численный метод, позволяющий применять единые позиционные характеристики (ПК) как при обратном преобразовании из МК в ПК, так и при коррекции ошибок вычислений. В качестве таких ПК целесообразно использовать коэффициенты позиционной весомозначной системы

счисления (ПВСС). Цель: разработать численный метод вычисления коэффициентов ПВСС, применение которого позволяет снизить схемные и временные затраты как при выполнении обратного преобразования, так и при коррекции ошибки в модулярном коде.

1. Модульные и немодульные операции ППМК

Полиалфавитный полиномиальный модулярный код – это непозиционный арифметический код. Основные принципы построения модулярного кода были разработаны М. Валахом и А. Свобода [8]. Развитие данной теории было продолжено как отечественными, так и зарубежными учеными [7, 8, 12 – 15]. Для получения кодовой комбинации ППМК выбираются неприводимые полиномы $p_1(x), \ldots, p_k(x)$, удовлетворяющие условию

$$deg\, p_1(x) \le deg\, p_2(x) \le \ldots \le deg\, p_k(x). \quad (1)$$

Тогда рабочий диапазон разрешенных КК равен

$$P_{\text{раб}}(x) = \prod_{i=1}^{k} p_i(x). \quad (2)$$

Если для полинома $A(x)$ выполняется условие:

$$deg\, A(x) < deg\, P_{\text{раб}}(x), \quad (3)$$

то КК полиномиального модулярного кода имеет вид

$$A(x) = A_1(x), A_2(x) \ldots, A_k(x)), \quad (4)$$

где $A(x) = A_i(x) mod\, p_i(x); i = 1, \ldots, k$.

Как отмечалось ранее, в ППМК модульные операции выполняются параллельно по основаниям кода:

$$A(x) \circ K(x) = |A_i(x) \circ K_i(x)|_{p_{i(x)}}, \quad (5)$$

где $\circ$ – модульные операции сложения, вычитания и умножения; $K(x) = K_i(x) mod\, p_i(x); i = 1, \ldots \ldots, k$.

Именно это свойство кодов было использовано при разработке высокоскоростных вычислительных систем [7, 8] и для повышения скорости аутентификации спутников [16,17].

Первой обязательной операцией для реализации вычислений в ППМК является прямое преобразование из ПК в ППМК. В работе [8] представлен последовательный алгоритм, а в работе [7] – алгоритм параллельного вычисления остатков. После проведения вычислений в ППМК необходимо полученный результат перевести в позиционный код. В настоящее время известны две реализации обратного преобразования [8]. При выполнении обратного преобразования ППМК–ПК часто используются ортогональные базисы:

$$B_i(x) = \frac{m_i(x) P_{\text{раб}}(x)}{p_i(x)} = m_i(x) P_i^*(x), \quad (6)$$

где $m_i(x) = |P_i^*(x))^{-1}|_{p_{i(x)}}$ – вес i-го ортогонального базиса; $i = 1, \ldots, k$.

Тогда для перевода ППМК–ПК справедливо

$$A(x) = \sum_{i=1}^{k} A_i(x) B_i(x) - r(x) P_{\text{раб}}(x), \quad (7)$$

где $r(x)$ – ранг полинома $A(x)$.

Основной недостаток перевода (7) состоит в том, что, как правило, $\deg \sum_{i=1}^{k} A_i(x) B_i(x) \ge \deg P_{\text{раб}}(x)$. Поэтому необходимо дополнительно вычислять ранг $r(x)$, чтобы выполнялось условие (3).

Данного недостатка лишено преобразование с использованием ПВСС. В этом случае полином $A(x)$ представляется в виде:

$$A(x) = C_1(x) + C_2(x) p_1(x) + \ldots + C_k(x) \prod_{j=1}^{k-1} p_j(x), \quad (8)$$

где $C_i(x)$ – коэффициенты ПВСС; $C_1(x) = A_1(x)$.

Анализ выражения (8) показывает, что при использовании ПВСС вычисленный полином $A(x)$ будет сразу удовлетворять условию (3). Если расширить кортеж оснований за счет введения контрольных модулей, то ПВСС можно использовать в процедуре коррекции ошибки вычислений. При этом процесс обнаружения и исправления ошибки можно выполнять при реализации преобразования ППМК–ПК. В этом случае ПВСС позволяет одновременно выполнить две эти операции, что положительно скажется на сокращении временных и схемных затратах при реализации спецпроцессора ППМК.

2. Избыточные полиалфавитные полиномиальные модулярные коды

Основой построения кодов, которые способны корректировать ошибки, является вводимая в КК избыточность [18, 19]. В результате КК содержит две части – информационную и проверочную. В большинстве избыточных ПК значение разрядов проверочной части КК определяются с помощью проверочных уравнений:

$$b_j = \lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_k a_k, \quad (9)$$

где a и b – соответственно информационные и проверочные разряды КК; $\lambda = \{0,1\}$ – определяется порождающей матрицей кода; $j = 1, \ldots, p$; k и ρ – количество информационных и проверочных разрядов в КК.

В результате полученные с помощью (9) избыточные коды нельзя использовать для выполнения вычислений. Поэтому они широко применяются в беспроводных системах передачи для повышения их помехоустойчивости [18].

Для того чтобы модулярные коды могли находить и исправлять ошибки вычислений, в КК вводится ρ дополнительных проверочных остатков:

$$A(x) = \left(A_1(x), \ldots, A_k(x), A_{k+1}(x), \ldots, A_{k+p}(x)\right). \quad (10)$$

Эти остатки получаются с помощью контрольных оснований $p_{k+1}(x), \ldots, p_{k+p}(x)$, для которых

$$deg\, p_k\,(x) \le deg\, p_{k+1}\,(x) \ldots \le deg\, p_{\,k+p}(x). \quad (11)$$

Введение этих оснований приводит к увеличению диапазона КК, которое задается полным диапазоном

$$P_{\text{пол}} = \prod_{i=1}^{k+p} p_i = P_{\text{раб}} \prod_{i=k+1}^{k+p} p_i. \quad (12)$$

Диапазон разрешенных КК ППМК определяется выражением (2). В этом случае избыточная КК (10) относится к разрешенным, если выполняется (3). Другими словами, в этом случае справедливо

$$H(x) = \left\lfloor A(x)/P_{\text{раб}}(x) \right\rfloor = 0. \quad (13)$$

С помощью выражения (13) вычисляется позиционная характеристика (ПХ) – полиномиальный интервал КК ППМК [20]. Согласно [7 – 9] однократной ошибкой в ППМК считается искажение одного остатка КК, т.е.

$$A_j^*(x) = (A_j(x) + \Delta A_j(x), \quad (14)$$

где $\Delta A_j(x)$ – глубина ошибки по j-му основанию; $j = 1, \ldots, k+p$.

В результате возникновения ошибки для КК будет нарушено условие (3) и справедливо неравенство

$$deg\, A^*\,(x) > deg\, P_{\text{раб}}\,(x). \quad (15)$$

В работе [9] описаны теоретические основы построения ППМК, способного корректировать однократные ошибки. В работе доказана теорема, определяющая вводимую избыточность для такого кода, согласно которой полиалфавитный полиномиальный модулярный код с двумя контрольными основаниями $p_{k+1}(x)$ и $p_{k+2}(x)$ способен исправить один искаженный остаток КК при условии:

$$deg(\, p_{k-1}(x) p_k(x)) \le deg(p_{k+1}(x) p_{k+2}(x)). \quad (16)$$

При доказательстве авторы использовали ПХ «полиномиальный интервал КК ППМК», которая вычисляется согласно (13). Между этой ПХ и коэффициентами ПВСС имеется связь.

Теорема 1. Если в избыточном полиалфавитном полиномиальном модулярном коде, имеющем контрольные основания, удовлетворяющие условию (16), произошла ошибка в одном остатке, то справедливо

$$H(x) = C_{k+1}^*(x) + C_{k+2}^*(x) p_{k+2}(x). \quad (17)$$

Доказательство.

При введении двух контрольных оснований полинома $A(x)$ в ПВСС будет определяться выражением:

$$A(x) = C_1(x) + C_2(x) p_1(x) + \ldots + C_k(x) \prod_{j=1}^{k-1} p_j\,(x) + C_{k+1}(x) P_{\text{раб}}(x) + C_{k+2}(x) P_{\text{раб}}(x) p_{k+1}(x). \quad (18)$$

Из выражения (18) наглядно видно, что если для избыточной КК (10) при $\rho = 2$ выполняется условие (3), то

$$C_{k+1}(x) = C_{k+2}(x) = 0. \quad (19)$$

При возникновении ошибки в КК выполняется условие (15), а значение ПХ «полиномиальный интервал КК ППМК» определяется как:

$$H(x) = \left\lfloor \Delta A_j(x) + B_j(x)/P_{\text{раб}}(x) \right\rfloor \neq 0, \quad (20)$$

где [*] – целая часть от деления.

В этом случае *выражение* (18) примет вид

$$A^*(x) = C_1^*(x) + C_2^*(x) p_1(x) + \ldots + C_k^*(x) \prod_{j=1}^{k-1} p_j\,(x) + C_{k+1}^*(x) P_{\text{раб}}(x) + C_{k+2}^*\,(x) P_{\text{раб}}(x) p_{k+1}(x). \quad (21)$$

Так как для ошибочной КК ППМК имеет место условие (15), то значения старших коэффициентов равно

$$C_{k+1}(x) \neq 0, C_{k+2}(x) \neq 0. \quad (22)$$

Разделим равенство (18) на рабочий диапазон и возьмем целую часть от результата. Получаем

$$\left\lfloor A^*(x)/P_{\text{раб}}(x)\right\rfloor = C^*_{k+1}(x) + C^*_{k+2}(x)p_{k+1}(x). \quad (23)$$

Таким образом, имеем

$$H(x) = C^*_{k+1}(x) + C^*_{k+2}(x)p_{k+1}(x). \quad (24)$$

Теорема доказана.

Таким образом, опираясь на теорему 2, доказанную в работе [9], можно сделать вывод – коэффициенты ПВСС можно использовать как для перевода из ППМК в ПК, так и при поиске и коррекции ошибок.

3. Разработка численного метода вычисления коэффициентов ПВСС

Проведем сравнительный анализ альтернативных численных методов вычисления коэффициентов ПВСС. В работе [15] описан численный метод, который включает следующие этапы:

1. Исходное значение полинома $A(x)$ делится на первое основание $p_1(x)$. Первый коэффициент ПВСС равен:

$$C_1(x) = rest(A(x)/p_1(x)). \quad (25)$$

2. Частное $A_1^{"}(x) = [A(x)/p_1(x)]$ делится на второе основание $p_2(x)$. Второй коэффициент ПВСС равен:

$$C_2(x) = rest(A_1^{"}(x)/p_2(x)). \quad (26)$$

3. Частное $A_2^{"}(x) = [A_1(x)/p_2(x)]$ делится на третье основание $p_3(x)$. Третий коэффициент ПВСС равен:

$$C_3(x) = rest(A_2^{"}(x)/p_3(x)). \quad (27)$$

4. Вычисления повторяются в течение k+2 этапов. При этом частное от деления на предыдущем шаге

$$C_i(x) = rest(A_{i-1}^{"}(x)/p_1(x)) \quad (28)$$

представляет собой i-й коэффициент ОПС.

В работе [20] представлен итерационный ЧМ вычисления коэффициентов ПВСС на основе КК ППМК:

$$\begin{aligned} &C_1(x) = A_1(x), C_2(x) = \left|\left(A_2(x) - C_1(x)\right)s_{12}(x)\right|^{+}_{p_{2(x)}},\\ &\vdots\\ &C_{k+2}(x) = (((((A_{k+2}(x) - C_1(x)s_{1(k+2)}(x) - \ldots - C_{k+1}(x))s_{(k+1)(k+2)}(x)), \end{aligned} \quad (29)$$

где $s_{ji}(x) = \left(\frac{1}{p_j(x)}\right) mod\ p_i(x); i.j = 1, \ldots, k+2; j \neq i.$

Основным недостатком данного ЧМ являются большие временные затраты на вычисления коэффициентов ПВСС. Модификация ЧМ вычисления коэффициентов ППВС, определяемого (29), представлена в [21]:

$$C_i(x) = \left\|A_i(x) - \sum_{j=1}^{i-1} C_j(x) \prod_{w=1}^{j} p_w(x)\right|_{p_{i(x)}} / \prod_{j=1}^{i-1} p_j(x)|_{p_{i(x)}}. \quad (30)$$

Снижение временных затрат при использовании ЧМ (30) достигается за счет предварительного вычисления констант, которые определяются произведением оснований ППМК.

Проведенный сравнительный анализ альтернативных решений выявил следующее противоречие в теории. Рассмотренные выше численные методы имеют итерационный характер. Так как коэффициенты вычисляются последовательно друг за другом, то при реализации этих ЧМ потребуются значительные временные затраты. При этом процесс разработки численных методов, позволяющих параллельно вычислять коэффициенты ПВСС, находится в стадии становления и еще далек от своего окончательного решения. Одним из решений данного противоречия является использование в ЧМ вычисления коэффициентов ПВСС Китайской теоремой об остатках (КТО) в полиномах. В данном методе ортогональные базисы представляются в виде коэффициентов ПВСС.

$$\begin{aligned} &B_1(x) = (1,\ C_2^1(x),\ C_3^1(x),\ \ldots, C_{k+1}^1(x), C_{k+2}^1(x)),\\ &B_2(x) = (0,\ C_2^2(x),\ C_3^2(x),\ \ldots, C_{k+1}^2(x), C_{k+2}^2(x)),\\ &\vdots\\ &\mathrm{B}_{k+2}(x) = (0,\ 0,\ 0,\ \ldots,\ 0, C_{k+2}^{k+2}(x)). \end{aligned} \quad (31)$$

Для вычисления коэффициентов ПВСС сначала остатки КК ППМК умножаются на ортогональные базисы.

$$\begin{aligned} &A_1(x)B_1(x) = (A_1(x),\ A_1(x)C_2^1(x),\ \ldots, A_1(x)C_{k+2}^1(x)),\\ &A_2(x)B_2(x) = (0,\ A_2(x)C_2^2(x),\ \ldots, A_2(x)C_{k+2}^2(x)),\\ &\vdots\\ &A_{k+2}(x)\mathrm{B}_{k+2}(x) = (0,\ 0,\ 0,\ \ldots,\ 0, A_{k+2}(x)\mathrm{C}_{k+2}^{k+2}(x)). \end{aligned} \quad (32)$$

Операция умножения остатков на соответствующие коэффициенты ПВСС выполняются по основанию ППМК, учитывая при этом количество превышений величины этого основания, которое представляется в виде полинома превышений контрольного основания $\mu(x)$. Если полученные результаты выражения (32) представить в виде таблицы, то для получения i-го коэффициента ПВСС необходимо сложить по модулю два произведения, которые находятся i-м столбце. Эти произведения были получены по модулю $p_1(x)$. При этом необходимо к полученному результату прибавить по модулю два превышения контрольного основания $\mu_{i-1}(x)$.

Так, первый коэффициент ПВСС равен

$$C_1(x) = A_1(x) \cdot 1 = A_1(x). \tag{33}$$

Значение второго коэффициента определяется как

$$C_2(x) = |A_1(x)C_2^1(x) + A_2(x)C_2^2(x)|_{p_2(x)}. \tag{34}$$

Пусть степень произведений в выражении (34) больше или равна степени основания $p_2(x)$. В этом случае частное при делении этого произведения на основание $p_2(x)$ в полиномиальной форме буден $\mu_2(x) \neq 0$. Тогда третий коэффициент ПВСС вычисляется как

$$C_3(x) = A_1(x)C_3^1(x) + A_2(x)C_3^2(x) + A_3(x)C_3^3(x) + \mu_2(x)\mathrm{mod}p_3(x) = \left|\sum_{i=1}^{3} A_i(x)C_3^i + \mu_2(x)\right|_{p_3(x)}. \tag{35}$$

Первый старший коэффициент ПВСС вычисляется как

$$C_{k+1}(x) = \left|\sum_{i=1}^{k+1} A_i(x)C_{k+1}^i + \mu_k(x)\right|_{p_{k+1}(x)}. \tag{36}$$

Второй старший коэффициент ПВСС вычисляется с учетом превышений контрольного основания $\mu_{k+1}(x)$,

$$C_{k+2}(x) = \left|\sum_{i=1}^{k+2} A_i(x)C_{k+2}^i + \mu_{k+1}(x)\right|_{p_{k+2}(x)}. \tag{37}$$

При реализации данного ЧМ операцию умножения остатков на коэффициенты ортогональных базисов можно выполнить одновременно за один такт, если использовать табличную реализацию (LUT-таблицы). После этого для вычисления коэффициента $C_{k+2}(x)$ требуется выполнить $k+3$ операции сложения.

Для сокращения временных и схемных затрат на выполнение преобразование ППМК–ПК был разработан численный метод вычисления коэффициентов ПВСС. В основу этого метода положен изоморфизм КТО в полиномах. Вместо МК с двумя с контрольными основаниями $p_{k+1}(x)$ и $p_{k+2}(x)$ возьмем два кода, имеющих минимальную избыточность. Оба кода имеют одинаковый кортеж информационных оснований $p_1(x), p_1(x), \ldots, p_k(x)$. При этом в первом коде контрольным полиномом выбран $\dot{p}_{k+1}(x) = p_{k+1}$, а во втором – $\ddot{p}_{k+1}(x) = p_{k+2}(x)$. Вычислим для кодов ортогональные базисы и представим их в виде коэффициентов ПВСС. Для кода с контрольным основанием $\dot{p}_{k+1}(x)$ имеем:

$$\begin{aligned}
&\dot{B}_1(x) = (1,\ \dot{C}_2^1(x),\ \dot{C}_3^1(x),\ \ldots,\ \dot{C}_k^1(x),\ \dot{C}_{k+1}^1(x)),\\
&\dot{B}_2(x) = (0,\ \dot{C}_2^2(x),\ \dot{C}_3^2(x),\ \ldots,\ \dot{C}_k^2(x),\ \dot{C}_{k+1}^2(x)),\\
&\vdots\\
&\dot{B}_k(x) = (0,\ 0,\ 0,\ \ldots,\ \dot{C}_k^k(x),\ \dot{C}_{k+1}^k(x)),\\
&\dot{B}_{k+1}(x) = (0,\ 0,\ 0,\ \ldots,\ 0,\ \dot{C}_{k+1}^{k+1}(x)).
\end{aligned} \tag{38}$$

Для второго кода с основанием $\ddot{p}_{k+1}(x)$ имеем:

$$\begin{aligned}
&\ddot{B}_1(x) = (1,\ \ddot{C}_2^1(x),\ \ddot{C}_3^1(x),\ \ldots,\ \ddot{C}_k^1(x),\ \ddot{C}_{k+1}^1(x)),\\
&\ddot{B}_2(x) = (0,\ \ddot{C}_2^2(x),\ \ddot{C}_3^2(x),\ \ldots,\ \ddot{C}_k^2(x),\ \ddot{C}_{k+1}^2(x)),\\
&\vdots\\
&\ddot{\mathrm{B}}_k(x) = (0,\ 0,\ 0,\ \ldots,\ \ddot{C}_k^k(x),\ \ddot{C}_{k+1}^k(x)),\\
&\ddot{\mathrm{B}}_{k+1}(x) = (0,\ 0,\ 0,\ \ldots,\ 0,\ \ddot{C}_{k+1}^k(x)).
\end{aligned} \tag{39}$$

Так как наборы информационных оснований в этих кодах одинаковые, то квадратные матрицы размером $k \times k$ коэффициентов ПВСС в выражениях (38) и (39) совпадают. То есть

$$\begin{aligned}
&\left(1\dot{C}_2^1(x), \dot{C}_3^1(x) \ldots \dot{C}_k^1(x)\right) = \left(1, \ddot{C}_2^1(x), \ddot{C}_3^1(x) \ldots \ddot{C}_k^1(x)\right),\\
&\left(0, \dot{C}_2^2(x)\dot{C}_3^2(x) \ldots \dot{C}_k^2(x)\right) = \left(0, \ddot{C}_2^2(x)\ddot{C}_3^2(x) \ldots \ddot{C}_k^2(x)\right),\\
&\vdots\\
&\left(0, 0, 0, \ldots \dot{C}_k^k(x)\right) = \left(0, 0, 0, \ldots \ddot{C}_k^k(x)\right).
\end{aligned} \tag{40}$$

Выражения (38) и (39) отличаются друг от друга только последними столбцами коэффициентов ПВСС, которые соответствуют контрольным основаниям ППМК. Значит, в разработанном ЧМ вычисление k первых коэффициентов ПВСС можно осуществлять с помощью коэффициентов ортогональных базисов (40). Тогда

$$C_j(x) = \sum_{i=1}^{j} A_i(x)\dot{C}_i^j(x) + \mu_{i-1}(x) \bmod p_j(x), \quad (41)$$

где $j = 1, \ldots, k$.

После этого выполняется параллельное вычисление двух старших коэффициентов ПВСС $\dot{C}_{k+1}(x)$ и $\ddot{C}_{k+1}(x)$.

$$\dot{C}_{k+1}(x) = \sum_{i=1}^{k+1} A_i(x)\dot{C}_i^{k+1}(x) + \mu_k(x) \bmod \dot{p}_{k+1}(x). \quad (42)$$

$$\ddot{C}_{k+1}(x) = \sum_{i=1}^{k+1} A_i(x)\ddot{C}_i^{k+1}(x) + \mu_k(x) \bmod \ddot{p}_{k+1}(x). \quad (43)$$

Коррекция осуществляется следующим образом. На основе ненулевых коэффициентов $\dot{C}_{k+1}(x), \ddot{C}_{k+1}(x)$ вычисляется вектор ошибки $\bar{e} = (\Delta C_1(x), \ldots, \Delta C_k(x))$. Затем происходит коррекция k коэффициентов ПВСС:

$$C_i(x) = (C_i^*(x) + \Delta C_i(x)), \quad (44)$$

где $i = 1, \ldots, k$.

После этого, используя исправленные коэффициенты ПВСС, вычисляется полином согласно (8).

Анализ выражений (42) и (43) показывает, что в разработанном ЧМ для вычисления $\dot{C}_{k+1}(x)$ и $\ddot{C}_{k+1}(x)$ требуется выполнить $k + 2$ операции сложения. При этом в отличие от ЧМ (33 – 37) количество переносов $\mu_i(x)$ будет уменьшено на единицу, что также способствует сокращению временных затрат на вычисление коэффициентов ПВСС. Кроме того, разработанный численный метод позволяет сократить схемные затраты. Так, при использовании ЧМ (33 – 37) для вычисления коэффициента $C_{k+1}(x)$ при табличной реализации требуется $k + 1$ LUT-таблицы, в которых хранятся результаты умножения остатков $A_i(x)C_{k+1}^i mod\ p_{k+1}(x)$, , где $i = 1, \ldots, k$. А для вычисления коэффициента $C_{k+1}(x)$ при табличной реализации требуется $k + 2$ LUT-таблицы. В разработанном численном методе для вычисления $\dot{C}_{k+1}(x)$ и $\ddot{C}_{k+1}(x)$ требуется $k + 1$ LUT-таблицы.

4. Результаты исследования и их обсуждение

Проведем сравнительный анализ временных и схемных затрат, необходимых на выполнение разработанного численного метода и ЧМ, определяемого выражениями (33 – 37). Для разработанного ЧМ выберем в качестве информационных оснований многочлены $p_1(x) = x + 1$, $p_2(x) = x^2 + x + 1$, $p_3(x) = x^4 + x^3 + x^2 + x + 1$, а в качестве контрольных $\dot{p}_4(x) = x^4 + x^3 + 1$ и $\dot{p}_4(x) = x^4 + x + 1$ соответственно для первого и второго кода. Для компактной записи воспользуемся шестнадцатеричной системой счисления. Тогда рабочий диапазон разрешенных КК определяется выражением (2), и он равен $P_{\text{раб}}(x) = x^7 + x^6 + x^5 + x^2 + x + 1 = E7$. Вычислим ортогональные базисы первого кода, для которого полный диапазон равен $\dot{P}_{\text{раб}}(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1 = 9AF$, и представим их в виде коэффициентов ПВСС:

$$\dot{B}_1(x) = 765 = (1, 2, A, 8),$$
$$\dot{B}_2(x) = 672 = (0, 2, D, B),$$
$$\dot{B}_3(x) = 344 = (0, 0, 7, 5),$$
$$\dot{B}_4(x) = 252 = (0, 0, 0, 6).$$

Выбираем $A(x) = x^5 + x^3 + 1 = (1,3,8,2)$, удовлетворяющий (3). Вычислим коэффициенты ПВСС согласно (38):

$$\begin{aligned} &\dot{B}_1(x) \cdot 1 = (1 \cdot 1, 2 \cdot 1, A \cdot 1, 8 \cdot 1), \\ &\dot{B}_2(x) \cdot 3 = (0, 2 \cdot 3, \mathrm{D} \cdot 3, B \cdot 3), \\ &\dot{B}_3(x) \cdot 8 = (0, 0, 7 \cdot 8, 5 \cdot 8), \\ &\dot{B}_4(x) \cdot 2 = (0, 0, 0, 6 \cdot 2). \end{aligned} \quad (45)$$

Первый коэффициент равен $\dot{C}_1(x) = A_1(x) = 1$.

Для вычисления $\dot{C}_1(x)$ сложим по модулю два произведения второго столбца равенства (45)

$$\dot{C}_2(x) = |1 \cdot x + (x + 1) \cdot x|_{x^2+x+1} = |x + 1|_{x^2+x+1} = x + 1 = 3.$$

При вычислении второго произведения был получен полином $(x + 1)x = x^2 + x$, степень которого равна степени $p_2(x) = x^2 + x + 1$. В этом случае $\mu_2^2(x) = 1$. Для вычисления третьего коэффициента ПВСС сложим по модулю два произведения третьего столбца (44) и $\mu_2^2(x)$. Тогда согласно (41) имеем

$$\dot{C}_3(x) =$$
$$= \left((x^3 + x) \cdot 1 + (x^3 + x^2 + 1) \cdot (x + 1) + (x^2 + x + 1) \cdot x^3 + 1\right) mod\ x^4 + x^3 + x^2 + x + 1 = x^2 + 1 = 5.$$

При умножении остатка $A_2(x) = 3$ на $C_3^2(x) = D$ был получен полином $(x^3 + x^2 + 1)(x + 1) = x^4 + x^2 + x + 1$.

При делении этого полинома на $p_3(x)$ получили частное $\mu_3^2(x) = 1$. Аналогично было вычислено превышение основания $p_3(x)$ при умножении остатка $A_3(x) = 8$ на коэффициент $C_3^3(x) = 7$. В результате $\mu_3^3(x) = x$.

Для вычисления старшего коэффициента ПВСС воспользуемся выражением (42).

$$\dot{C}_4(x) = (x^3 \cdot 1 + (x^3 + x + 1) \cdot (x + 1) + (x^2 + 1) \cdot x^3 + (x^2 + x) \cdot x + 1 + x) mod\ x^4 + x^3 + 1 = 0.$$

Вычислим ортогональные базисы второго кода, для которого полный диапазон равен

$\ddot{P}_{\text{пол}}(x) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1 = F59.$

Представим их в виде коэффициентов ПВСС:

$\ddot{B}_1(x) = 537 = (1,2,A,E),$
$\ddot{B}_2(x) = 695 = (0,2,D,A),$
$\ddot{B}_3(x) = 116 = (0,0,7,3),$
$\ddot{B}_4(x) = 2B5 = (0,0,0,7).$

В качестве КК выбираем $A(x) = x^5 + x^3 + 1 = (1,3,8,F)$. Вычислим коэффициенты ПВСС согласно (39):

$$\begin{aligned}&\ddot{B}_1(x)\cdot 1 = (1\cdot 1, 2\cdot 1, A\cdot 1, 8\cdot 1),\\ &\ddot{B}_2(x)\cdot 3 = (0,2\cdot 3, D\cdot 3, B\cdot 3),\\ &\ddot{B}_3(x)\cdot 8 = (0,0,7\cdot 8, 5\cdot 8),\\ &\ddot{B}_4(x)\cdot F = (0,0,0,6\cdot F).\end{aligned} \quad (46)$$

Так как выполняется равенство (40), то для первых трех коэффициентов ПВСС справедливо, $\dot{C}_1(x) = \ddot{C}_1(x) = 1$, $\dot{C}_2(x) = \ddot{C}_2(x) = 3$, $\dot{C}_3(x) = \ddot{C}_3(x) = 5$.

Воспользуемся выражением (43) и вычислим старший коэффициент ПВСС для второго кода:

$\ddot{C}_4(x) = \big((x^3 + x^2 + x)\cdot 1 + (x^3 + x)\cdot(x+1) + (x+1)\cdot x^3 + (x^2 + x + 1)\cdot(x^3 + x^2 + x + 1) + 1 + x\big) mod\ x^4 + x + 1 = 0.$

Так как $\dot{C}_4(x) = \ddot{C}_4(x) = 0$, то кодовая комбинация ППМК не содержит ошибочных остатков и можно ее переводить в ПК. Для этого воспользуемся (8):

$$A(x) = C_1(x) + C_2(x)p_1(x) + C_3(x)p_1(x)p_2(x) = 1 + (x+1)(x+1) + (x^2+1)(x^3+1) = x^5 + x^3 + 1.$$

Пусть в КК произошла ошибка во втором остатке с глубиной $\Delta A_2(x) = x$. Согласно (14) имеем

$A_2^*(x) = A_2(x) + \Delta A_2(x) = (x+1) + x = 1.$

Запрещенная КК для первого кода имеет вид $A^*(x) = (1, 1^*, 8, 2)$. Вычислим коэффициенты ПВСС согласно (38).

$\dot{B}_1(x)\cdot 1 = (1\cdot 1,\ 2\cdot 1,\ A\cdot 1,\ 8\cdot 1),$
$\dot{B}_2(x)\cdot 1^* = (0,\ 2\cdot 1^*,\ D\cdot 1^*, B\cdot 1^*),$
$\dot{B}_3(x)\cdot 8 = (0,\ 0,\ 7\cdot 8,\ 5\cdot 8),$
$\dot{B}_4(x)\cdot 2 = (0,\ 0,\ 0,\ 6\cdot 2).$

Согласно (41) получаем следующие коэффициенты ПВСС. Первый коэффициент равен $\dot{C}_1(x) = A_1(x) = 1$. Значение второго коэффициента равно

$\dot{C}_2(x) = |1\cdot x + 1\cdot x|_{x^2+x+1} = 0.$

При этом переносов в старшие коэффициенты не происходит. Значение третьего коэффициента равно

$\dot{C}_3(x) = \big((x^3 + x)\cdot 1 + (x^3 + x^2 + 1)\cdot 1\big) + (x^2 + x + 1)\cdot x^3\big) mod\ x^4 + x^3 + x^2 + x + 1 = 1.$

При этом $\mu_3^3(x) = x$. Согласно (42) старший коэффициент ПВСС равен

$\dot{C}_4(x) = (x^3\cdot 1 + (x^3 + x + 1)\cdot 1 + (x^2+1)\cdot x^3 + (x^2 + x)\cdot x + x) mod\ x^4 + x^3 + 1 = x^3 + x^2 + x = E.$

Произведем вычисление старшего коэффициента ПВСС для второго кода. В этом случае КК имеет вид $A^*(x) = (1, 1^*, 8, F)$. Согласно (43) имеем

$\ddot{C}_4(x) = \big((x^3 + x^2 + x)\cdot 1 + (x^3 + x)\cdot 1 + (x+1)\cdot x^3 + (x^2 + x + 1)\cdot(x^3 + x^2 + x + 1) + 1 + x\big) mod\ x^4 + x + 1 = x^2 + x = 6.$

Полученные коэффициенты $\dot{C}_4(x) = E, \ddot{C}_4(x) = 6$ показывают, что в КК ППМК присутствует ошибка, которой соответствует вектор ошибки $\bar{e} = (0, x+1, x^2)$. Воспользуемся выражением (44) для ее коррекции:

$A(x) = A^*(x) + \bar{e}(x) = [1+0, 0 + (x+1), 1 + x^2] = [1, x+1, x^2+1].$

Рассмотрим численный метод вычисления коэффициентов ПВСС, определяемый выражениями (33 – 37). Набор информационных и контрольных оснований оставляем прежний. В этом случае полный диапазон избыточного ППМК равен $P_{\text{пол}}(x) = x^{15} + 1 = 1000000000000001 = 8001$. Вычислим ортогональные базисы

$B_1(x) = 7FFF = (1, 2, A, 8, E)$,
$B_2(x) = 6DB6 = (0, 2, D, B, C)$,
$B_3(x) = 7BDE = (0, 0, 7, 5, E)$,
$B_4(x) = 7AC8 = (0, 0, 0, 6, E)$,
$B_5(x) = 135E = (0, 0, 0, 0, 2)$.

Выберем полином $A(x) = x^5 + x^3 + 1 = (1, x + 1, x^3, x, x^3 + x^2 + x + 1) = (1,3,8,2,F)$, который удовлетворяет условию (3). Для вычисления коэффициентов ПВСС умножим остатки КК ППМК на ортогональные базисы, представленные в ПВСС согласно (32). Получаем

$B_1(x) \cdot 1 = (1 \cdot 1,\ 2 \cdot 1,\ A \cdot 1, 8 \cdot 1,\ E \cdot 1)$,
$B_2(x) \cdot 3 = (0,\ 2 \cdot 3,\ D \cdot 3, B \cdot 3, C \cdot 3)$,
$B_3(x) \cdot 8 = (0,\ 0,\ 7 \cdot 8,\ 5 \cdot 8,\ E \cdot 8)$, (47)
$B_4(x) \cdot 3 = (0,\ 0,\ 0,\ 6 \cdot 2,\ E \cdot 2)$,
$B_5(x) \cdot F = (0,\ 0,\ 0,\ 0,\ 2 \cdot F)$.

Первый коэффициент равен $C_1(x) = A_1(x) = 1$.

Для вычисления $C_2(x)$ сложим по модулю два произведения второго столбца равенства (47). Представив коэффициенты ПВВС и остатки в виде полиномов $2 = x, 3 = x + 1$, согласно (34) получаем

$$C_2(x) = |1 \cdot x + (x + 1) \cdot x|_{x^2+x+1} = |x + 1|_{x^2+x+1} = x + 1 = 3.$$

При вычислении второго произведения был получен полином $(x + 1)x = x^2 + x$, степень которого равна степени $p_2(x) = x^2 + x + 1$. В этом случае $\mu_2^2(x) = 1$.

Для вычисления третьего коэффициента ПВСС сложим по модулю два произведения третьего столбца (47) и $\mu_2^2(x)$. Тогда согласно (35) имеем

$$C_3(x) = \\ = \left((x^3 + x) \cdot 1 + (x^3 + x^2 + 1) \cdot (x + 1) + (x^2 + x + 1) \cdot x^3 + 1\right) mod\ x^4 + x^3 + x^2 + x + 1 = x^2 + 1 = 5.$$

При умножении остатка $A_2\ (x) = 3$ на $C_3^2 = D$ был получен полином $(x^3 + x^2 + 1)(x + 1) = x^4 + x^2 + x + 1$. При делении этого полинома на $p_3(x)$ получили частное $\mu_3^2(x) = 1$. Аналогично было вычислено превышение основания $p_3(x)$ при умножении остатка $A_3\ (x) = 8$ на коэффициент $C_3^3 = 7$. В результате получили $\mu_3^3(x) = x$. Для вычисления четвертого коэффициента ПВСС сложим по модулю два произведения четвертого столбца (47) и два переполнения $\mu_3^2(x)$, $\mu_3^3(x)$ Тогда

$$C_4(x) = (x^3\ \cdot 1 + (x^3 + x + 1) \cdot (x + 1) + (x^2 + 1) \cdot x^3 + (x^2 + x) \cdot x + 1) mod\ x^4 + x^3 + 1 = 0.$$

Для вычисления пятого коэффициента ПВСС сложим по модулю два произведения пятого столбца (47), и $\mu_4^2(x) = 1$, $\mu_4^3(x) = x + 1$. Тогда

$$C_5(x) = ((x^3 + x^2 + x) \cdot 1 + (x^3 + x^2)(x + 1) + (x^3 + x^2 + x)x^3 + (x^3 + x^2 + x)x + \\ + x(x^3 + x^2 + x + 1) + 1 + (x + 1)) mod x^4 + x + 1 = 0.$$

Так как $C_4(x) = C_5(x) = 0$, то это значит, что КК является разрешенной и не содержит ошибки.

Результаты исследования показали, что для вычисления коэффициента $C_5(x)$ при использовании численного метода (33 – 37) понадобилось выполнить 5 операций умножения и 6 операций сложения по модулю два. При использовании разработанного численного метода для вычисления старшего коэффициента потребовалось 4 операции умножения и 5 операций сложения по модулю два. Таким образом, за счет использования в разработанном численном методе изоморфизма КТО в 1,25 раза сокращено количество операций умножения и в 1,2 раза операций сложения. При этом для вычисления коэффициента $C_5(x)$ при использовании ЧМ (33 – 37) понадобилось пять LUT-таблиц, а в разработанном ЧМ – четыре LUT-таблицы, то есть схемные затраты были сокращены в 1,25 раза. Таким образом, цель исследований достигнута.

Заключение

Применение МК позволяет повысить производительность систем ЦОС за счет распараллеливания вычислений на уровне выполнения арифметических операций. Кроме этого, при введении в них избыточности модулярные коды способны обнаруживать и корректировать ошибки вычислений. Однако это негативно сказывается на схемных затратах и производительности систем ЦОС, так как процесс поиска и исправления ошибок выполняется независимо от обязательной процедуры обратного преобразования из МК в ПК. Для устранения этого противоречия в статье было предложено воспользоваться коэффициентами ПВСС, которые применяются как при выполнении обратного преобразования, так и в процедурах коррекции ошибок. На основе проведенного сравнительного анализа альтернативных численных методов вычисления коэффициентов ПВСС было показано противоречие в теории. Для устранения этого противоречия был разработан численный метод, отличающийся от ранее известных использованием изоморфизма КТО в полиномах при вычислении

коэффициентов ПВСС непосредственно из кодовой комбинации полиалфавитного полиномиального модулярного кода. Проведенный сравнительный анализ показал, что для реализации разработанного ЧМ при использовании трех информационных и двух контрольных оснований ППМК требуется в 1,25 раз меньше схемных затрат по сравнению численным методом (33 – 37). При этом за счет использования изоморфизма КТО в 1,25 раза сокращено количество операций умножения и в 1,2 раза операций сложения.

Благодарности

Исследование выполнено за счет гранта Российского научного фонда № 25-71-30007, https://rscf.ru/project/25-71-30007/

References

[1] Sazanov VM, Parfenov NS. Digital signal processing: past and present. Electronic resource. Virtual computer museum. Source: <http://www.computer-museum.ru//histussr/dsp.htm>.
[2] Murthy CS, Sridevi K. FPGA implementation of high speed-low energy RNS based reconfigurable-FIR filter for cognitive radio applications. WSEAS Trans. Syst. Control 2021; 16: 278–293. DOI: 10.37394/23203.2021.16.24.
[3] Chang C-H, Molahosseini AS, E. Zarandi A A, Tay TF. Residue Number Systems: A New Paradigm to Datapath Optimization for Low-Power and High-Performance Digital Signal Processing Applications. *IEEE Circuits and Systems Magazine,* Fourthquarter 2015; 15(4): 26-44. DOI:10.1109/MCAS.2015.2484118.
[4] Srinivasa CM, Sridevi K. FPGA Implementation of High Speed-low Energy RNS based Reconfigurable-FIR Filter for Cognitive Radio Applications, WSEAS Transactions on Systems and Control, 2021; 16: 278-293. DOI: 10.37394/23203.2021.16.24.
[5] Rudramuniyappa H, Soujanya S. Optimized Algorithms for FPGA Implementation of PDCCH Chain for 5G-NR Base Station. IEEE Transactions on Circuits and Systems, 2025; 72(7): 3474 – 3487. DOI: 10.1109/TCSI.2024.3519752
[6] Balaji M, Padmaja N. Area and delay efficient RNS-based FIR filter design using fast multipliers. Measurement: Sensors, 2024; 31: 101014. DOI: 10.1016/j.measen.2023.101014.
[7] Ananda Mohan PV, Residue Number Systems. Theory and Applications. Switzerland: Springer International Publishing, 2016. ISBN: 978-3-319-41385-3.
[8] Omondi A, Premkumar B. Residue Number Systems: Theory and Implementation. UK: Imperial College Press, 2007. ISBN: 978-1-86094-866-4.
[9] Kalmykov IA, Olenev AA, Kononova NV, Peleshenko TA, Chistousov NK. A numerical method for parallel calculation of the positional characteristic for error correction in a polyalphabetic polynomial modular code. Computer Optics 2025; 49(1): 141-150. DOI: 10.18287/2412-6179-CO-1505.
[10] Kononova NV, Peleshenko TA, Dukhovnyj DV, Chistousov NK, Kalmykova NI. Improvement of the Cybersecurity of the Satellite Internet of Vehicles through the Application of an Authentication Protocol Based on a Modular Error-Correction Code. World Electr. Veh. J. 2024; 15: 278. DOI: 10.3390/wevj15070278.
[11] Valach M, Svoboda A. Origin of the Code and Number System of Remainder Classes. Stroje Na Zpracovani Informaci. Sbornik. 1955. Vol. 3.
[12] Akushsky IYa, Yuditsky DI. Machine arithmetic in residual classes [In Russian]. Moscow: “Sov. Radio” Publisher; 1968.
[13] Amerbaev VM, Pak IT, Parallel computing in the complex plane. AlmaAta: "Nauka" Publisher; 1984.
[14] Molahosseini AS. Embedded Systems Design with Special Arithmetic and Number Systems. Switzerland: Springer International Publishing AG; 2017. ISBN: 978-3-319-49741-9.
[15] Chervyakov NI, Shaposhnikov AV, Sakhnyuk PA, Makokha AN. ed. [In Russian]. Neurocomputers in residual classes. Moscow: “Radio engineering” Publisher; 2003. ISBN: 5-93108-054-6.
[16] Kalmykov IA, Olenev AA, Dukhovnyj DV, Provornov IA, Slyadnev VS. A Method for Fault Tolerance of AES Encryption Systems Focused on Improving the Cybersecurity of VANET Through the Use of Residue Codes. World Electr. Veh. J. 2025; 16: 462. DOI: 10.3390/wevj16080462.
[17] Kopytov VV, Olenev AA. Application of Modular Residue Classes Codes in an Authentication Protocol for Satellite Internet Systems. IEEE Access 2023; 11(1-1): 71624 – 71633. DOI: 10.1109/ACCESS.2023.3290498.
[18] Bierbrauer J. Introduction to coding theory. New York: Chapman and Hall/CRC, 2016. ISBN: 9781315371993. DOI: 9781315371993.
[19] Berlekamp ER. Algebraic Coding Theory - Revised Edition. World Scientific Publishing Co., Inc., USA. 2015. ISBN: 978-981-4635-89-9.
[20] Bajard J-C, Didier L-S, Kornerup P. Modular multiplication and base extension in residue number systems. In L. Ciminiera N. Burgess, editor, 15th IEEE Symposium on Computer Arithmetic, pages 59–65, Vail Colorado, USA, 2001. IEEE Computer Society Press. DOI: 10.1109/ARITH.2001.930104.
[21] Bajard J-C, Plantard T. RNS bases and conversions. Proc. SPIE 5559, Advanced Signal Processing Algorithms, Architectures, and Implementations XIV, 2004. DOI: 10.1117/12.557891.

Сведения об авторах

Калмыков Игорь Анатольевич, 1967 года рождения, профессор кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета. В 1989 году окончил Ставропольское высшее военное инженерное училище связи (СВВИУС). В 2006 году защитил диссертацию на соискание степени доктора технических наук. Сфера научных интересов: непозиционные системы счисления, параллельные вычисления, цифровая обработка сигналов, отказоустойчивые вычислительные системы. E-mail: *kia762@yandex.ru*

Оленев Александр Анатольевич, 1963 года рождения, старший научный сотрудник Института цифрового развития Северо-Кавказского федерального университета. В 1985 году окончил Ставропольское высшее военное инженерное училище связи. В 1993 году защитил диссертацию на соискание степени кандидата технических наук. Сфера научных интересов: непозиционные системы счисления, отказоустойчивые вычислительные системы, математическая логика. E-mail: olenevalexandr@gmail.com

Пелешенко Татьяна Александровна, 1992 года рождения, доцент кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета. В 2014 г. с отличием окончила обучение в Северо-Кавказском федеральном университете. В 2019 году защитила диссертацию на соискание ученой степени кандидата технических наук. Сфера научных интересов: непозиционные системы счисления, математические модели цифровой обработки сигналов на основе построения вейвлет-преобразований в конечных полях, методы и алгоритмы вейвлет-анализа для цифровой обработки сигналов. E-mail: gtanya09@mail.ru

Чистоусов Никита Константинович, 1995 года рождения, старший научный сотрудник Института цифрового развития Северо-Кавказского федерального университета. Получил в 2018 году степень специалиста (с отличием) по информационной безопасности автоматизированных систем Северо-Кавказского федерального университета (ИБАС СКФУ). В 2023 году защитил диссертацию на соискание степени кандидата технических наук. Сфера научных интересов: криптографические методы защиты информации, протоколы аутентификации с нулевым разглашением, непозиционные системы счисления. E-mail: chistousov.nik@yandex.ru

Фоменко Кирилл Сергеевич, 2001 года рождения, аспирант факультета математики и компьютерных наук имени профессора Н.И. Червякова. В 2025 году окончил Северо-Кавказский федеральный университет по специальности «Информационная безопасность автоматизированных систем». Сфера научных интересов: модулярные коды, цифровая обработка сигналов, технология OFDM, построение арифметических корректирующих кодов. E-mail: icekirill534@gmail.com

Поступила в редакцию 13 октября 2025 г. *Окончательный вариант – 16 декабря 2025 г.*

A numerical method for calculating coefficients of a positional weight-valued number system for performing the inverse transform and error correction in a modular code

I.A. Kalmykov [1], A.A. Olenev [1], T.A. Peleshenko [1] N.K. Chistousov [1], K.S. Fomenko [1]
[1] North Caucasus Federal State University, Pushkina Str. 1, Stavropol, 355017, Russia

Abstract

One of the effective methods of increasing the performance of digital signal processing systems is the use of parallel arithmetic codes, in particular, polyalphabetic polynomial modular codes. In these codes, performing modular operations (addition, subtraction, multiplication) requires less time compared to performing these operations in positional codes. This is achieved by independently executing these operations across code modules. However, such an organization of calculations requires a translation from positional codes to polyalphabetic polynomial modular codes, and after the calculations, performing the reverse translation. It is known that the latter operation requires quite a lot of time and circuit costs. To eliminate this problem, in this work, we develop a numerical method for calculating the coefficients of a positional weighty number system from a polyalphabetic polynomial modular code combination, which makes it possible to efficiently perform the reverse transformation. The coefficients obtained using this method can also be used to find and correct errors that occur during calculations in digital signal processing. The use of the isomorphism of the Chinese remainder Theorem has made it possible to reduce the time and circuit costs in calculating the coefficients of the positional weighty number system from the modular code.

Keywords: polyalphabetic polynomial modular codes, numerical methods, coefficients of a positional weight-valued number system, inverse transform, error correction in a modular code.

Citation: Kalmykov IA, Olenev AA, Peleshenko TA, Chistousov NK, Fomenko KS. A numerical method for calculating coefficients of a positional weight-valued number system for performing the inverse transform and error correction in a modular code. Computer Optics 2026; 50(4): 1857. DOI: 10.18287/COJ1857.

Acknowledgements: The research was financially supported by the Russian Science Foundation under grant No 25-71-30007, https://rscf.ru/en/project/25-71-30007.

About authors

Igor Anatolyevich Kalmykov, (b. 1967), Professor of the Department of Information Security of Automated Systems at the North Caucasus Federal University. In 1989, he graduated from the Stavropol Higher Military School of Communications. In 2006, he defended his dissertation for the degree of Doctor of Technical Sciences. Research interests: non-positional number systems, parallel computing, fault-tolerant computing systems. E-mail: *kia762@yandex.ru*

Aleksandr Anatolyevich Olenev, (b. 1963), Senior Researcher at the Institute of Digital Development of the North Caucasus Federal University. In 1985, he graduated from the Stavropol Higher Military School of Communications. In 1993, he defended his dissertation for the degree of Candidate of Technical Sciences. Research interests: non-positional number systems, fault-tolerant computing systems, mathematical logic. E-mail: *olene-valexandr@gmail.com*

Tatyana Alexandrovna Peleshenko, (b.1992), Associate Professor of the Department of Information Security of Automated Systems at the North Caucasus Federal University. In 2014, she graduated with honors from the NCFU. In 2019, she defended her dissertation for the degree of Candidate of Technical Sciences. Research interests: non-positional number systems, mathematical models of digital signal processing based on the construction of wavelet transformations in finite fields, methods and algorithms of wavelet analysis for digital signal processing. E-mail: *gtanya09@mail.ru*

Nikita Konstantinovich Chistousov, (b. 1995), Senior Researcher at the Institute of Digital Development of the North Caucasus Federal University. In 2018, he received a specialist's degree in information security of automated systems from the North Caucasus Federal University. In 2023, he defended his dissertation for the degree of Candidate of Technical Sciences. Research interests: cryptographic methods of information protection, zero-knowledge authentication protocols, non-positional number systems. E-mail: *chistousov.nik@yandex.ru*

Kirill Sergeevich Fomenko, (b. 2001), is a graduate student in the N.I. Chervyakov Faculty of Mathematics and Computer Science. He graduated from the North Caucasus Federal University in 2025 with a degree in information security for automated systems. His research interests include modular codes, digital signal processing, OFDM technology, and the construction of arithmetic-correcting codes. Email: *icekirill534@gmail.com*

Received October 13, 2025. The final version – December 16, 2025.