Численный метод параллельного вычисления позиционной характеристики для коррекции ошибок в полиалфавитном полиномиальном модулярном коде

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

Аннотация

Тенденция повышения эффективности вычислительных систем и устройств напрямую связана с переходом к параллельным вычислениям. Предлагается осуществлять параллельные вычисления на уровне арифметических операций, используя арифметические полиалфавитные модулярные коды, в которых кодовые комбинации представляют собой набор остатков, полученных при делении целого числа на основания. Различают два вида таких кодов. В полиалфавитном коде системы остаточных классов в качестве оснований используются взаимно простые числа. В полиалфавитном полиномиальном модулярном коде – неприводимые полиномы. Характерная черта этих кодов – выполнение операций сложения, вычитания и умножения параллельно по основаниям. Обмен данными между основаниями не производится. В результате достигается повышение производительности вычислительных систем. Основания полиалфавитных модулярных кодов равноправны, независимы и служат основой для построения арифметических кодов, обнаруживающих и исправляющих ошибки, возникающие в процессе вычислений. В статье представлены теоретические основы построения избыточных полиалфавитных полиномиальных модулярных кодов, способных обнаруживать и корректировать ошибки вычислений. На основе доказанных теорем был разработан численный метод вычисления позиционной характеристики полиномиального интервала в полиалфавитных полиномиальных модулярных кодах. Данный метод требует меньшего количества операций умножения по сравнению с классическим методом вычисления этой позиционной характеристики. Рассмотрены примеры применения данного метода.

Ключевые слова: параллельные вычисления, полиалфавитный полиномиальный модулярный код, контрольные основания, численный метод вычисления позиционной характеристики, коррекция ошибок.

Цитирование: **Калмыков, И.А.** Численный метод параллельного вычисления позиционной характеристики для коррекции ошибок в полиалфавитном полиномиальном модулярном коде / И.А. Калмыков, А.А. Оленев, Н.В. Кононова, Т.А. Пелешенко, Н.К. Чистоусов // Компьютерная оптика. – 2025. – Т. 49, № 1. – С. 141-150. – DOI: 10.18287/2412-6179-CO-1505.

Citation: 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.

Введение

Наблюдаемая в настоящее время тенденция к распараллеливанию вычислений связана с необходимостью решения многих практических задач в реальном масштабе времени. В статье рассматривается процесс распараллеливания, выполняемый на уровне арифметических операций, который эффективно реализуется на основе полиалфавитных модулярных кодов (ПМК). Так как в этих кодах кодовые комбинации представляют собой набор остатков, которые получены при делении целого числа на основания, то операции сложения, вычитания и умножения можно выполнять параллельно и независимо друг от друга. В результате этого повышается производительность вычислительных систем (ВС) [1 – 5]. Полиалфавитные модулярные коды являются непозиционными арифметическими кодами, в которых алфавиты остатков не совпадают друг с другом и определяются основаниями кода. Если в качестве оснований применяются взаимно простые целые числа, то получается полиалфавитный код системы остаточных классов (ПКСОК). Если в качестве оснований взять неприводимые полиномы, то получается полиалфавитный полиномиальный модулярный код (ППМК) [6, 7]. Так как вычисления в этих кодах выполняются параллельно с малоразрядными остатками, то ПКСОК и ППМК нашли применение в системах реального времени, в частности при цифровой обработке сигналов.

Однако широкое использование параллельных вычислительных систем способствовало появлению следующего противоречия. С одной стороны, посто-

янный рост требований к скоростным характеристикам ВС приводит к необходимости организации параллельных вычислений, а с другой стороны, при этом увеличивается частота возникновения отказов и возрастает время простоя процессоров, вызванного трудностью отыскания и ликвидации неисправности. Для решения данного противоречия была разработана теория построения корректирующих ПКСОК [2, 5, 6]. В отличие от помехоустойчивых кодов избыточные ПКСОК способны обнаруживать и исправлять ошибки, которые возникают в процессе вычислений. Для этого применяются позиционные характеристики (ПХ). Так как ошибка, возникшая по одному основанию, не может оказать влияние на другие основания, то обнаружение и коррекция ошибки производится в конце всех вычислений.

Однако несмотря на то, что принципы построения данных кодов подобны, теория обнаружения и коррекции ошибок в ППМК на основе использования ПХ находится в стадии становления и еще далека от своего окончательного решения. Актуальность решения данной задачи определяется тем, что разработка численного метода вычисления ПХ в ППМК позволит осуществлять коррекцию результатов линейного и нелинейного биективного преобразований, реализуемых в блочных SPN-шифрах. Благодаря этому будут устранены последствия атак «на основе сбоя», проводимых в шифрах AES и Кузнечик. Поэтому разработка численного метода вычисления ПХ для коррекции ошибок в полиалфавитном полиномиальном модулярном коде является актуальной задачей.

1. Арифметические принципы получения полиалфавитных модулярных кодов

Арифметические коды бывают позиционные и непозиционные. Среди последних особое место занимают ПМК, в которых базовые элементы кода генерируются на основе разных базисов (алфавитов) [7]. Началом развития теории построения ПМК считается работа чешского ученого Миро Валах [1], в которой для повышения скорости вычислений было предложено кодировать целые числа в кольце вычетов, которое было получено с помощью взаимно простых чисел. Базовые принципы модулярной арифметики были рассмотрены советскими учеными И.Я. Акушским и Д.И. Юдицким в [2]. Вопросы повышения скорости выполнения немодульных операций нашли отражение в работе В.М. Амербаева [3]. Повышение надежности вычислительных систем за счет применения модулярных кодов показано в работе В.А. Торгашова [6]. Современные исследователи [7 – 10] решают задачи по применению ПМК в цифровой обработке сигналов, фильтрации, криптографии, нейронных сетях. Основная цель данных исследований – повысить скорость вычислений и отказоустойчивость ВС за счет применения ПМК.

Если в качестве базисов такого кода выбрать числа $m_1, m_2, \ldots, m_k$, для которых выполняются

$$m_1 < m_2 < ... < m_k, \tag{1}$$

$$(m_i \ .m_j) = 1, \tag{2}$$

то получается полиалфавитный код системы остаточных классов. В этом случае кодовая комбинация целого числа S будет иметь вид

$$S = (s_1, s_2, ..., s_k), \tag{3}$$

где $S \equiv s_i, \bmod m_i$; $i = 1, \ldots, k$.

Для реализации вычислений в ПКСОК необходимо, чтобы операнды и результат вычисления не выходили за пределы рабочего диапазона

$$P_{раб} = \prod_{i=1}^{k} m_i \ . \tag{4}$$

Пусть заданы два целых числа S и G, тогда в ПКСОК можно выполнить аддитивные и мультипликативные арифметические операции [8, 9]

$$S + G = (s_1 + g_1 \bmod m_1, ..., s_k + g_k \bmod m_k), \tag{5}$$

$$S - G = (s_1 - g_1 \bmod m_1, ..., s_k - g_k \bmod m_k), \tag{6}$$

$$S \cdot G = (s_1 \cdot g_1 \bmod m_1, ..., s_k \cdot g_k \bmod m_k), \tag{7}$$

где $G \equiv g_i \bmod m_i$; $i = 1, \ldots, k$.

Если в качестве базисов полиалфавитного кода выбрать неприводимые полиномы $p_1(x), p_2(x), \ldots, p_k(x)$, для которых справедливо

$$\deg p_1(x) \le \deg p_2(x) \le ... \le \deg p_k(x), \tag{8}$$

то получается полиалфавитный полиномиальный модулярный код (ППМК) [6, 7]. В этом случае кодовая комбинация двоичного числа S будет иметь вид

$$S(x) = (s_1(x), s_2(x), ..., s_k(x)), \tag{9}$$

где $S(x)$ – полиномиальная форма числа S; $S(x) \equiv s_i(x) \bmod p_i(x)$; $i = 1, \ldots, k$.

Как и в ПКСОК, в данном коде необходимо, чтобы степень операндов и результатов вычисления не превышали степень рабочего диапазона

$$P_{раб}(x) = \prod_{i=1}^{k} p_i(x) \ . \tag{10}$$

Пусть заданы два полинома $S(x)$ и $G(x)$, тогда в ППМК можно выполнить модульные операции

$$\begin{aligned} &S(x) \circ G(x) = \\ &= \left| s_1(x) \circ g_1(x) \right|_{p_1(x)}, .., \left| s_k(x) \circ g_k(x) \right|_{p_k(x)}, \end{aligned} \tag{11}$$

где $\circ$ – модульные операции сложения, вычитания и умножения; $G(x) \equiv g_i(x) \bmod p_i(x)$; $i = 1, \ldots, k$.

Анализ равенств (5 – 7) и (11) показывает, что ППМК и ПСОК обладают одинаковыми достоинствами. Очевидно, что переход к вычислениям на основе полиалфавитных модулярных кодов позволяет увели-

чить скорость выполнения модульных операций. Данный положительный результат связан с тем, что:

- арифметические операции выполняются параллельно по базисам кода;
- операнды s_i, g_i имеют меньший размер по сравнению с числами S и G.

Поэтому полиалфавитные модулярные коды были применены в вычислительных системах реального времени, таких как спецпроцессоры цифровой обработки сигналов [8 – 10], цифровые фильтры [11 – 15], системы аутентификации низкоорбитальных спутников [16, 17], системы шифрования [18 – 20]. Так, в работе [20] представлена архитектура СБИС для реализации криптосистемы с открытым ключом RSA с использованием системы остаточных классов. Проведенные исследования показали, что использование ПСОК позволило увеличить скорость выполнения на 35 % по сравнению с существующими реализациями RSA.

Следует также отметить и другую особенность модулярных кодов. Равноправность и независимость оснований полиалфавитных модулярных кодов служит основой для построения арифметических кодов, способных обнаруживать и исправлять ошибки в процессе вычислений. В этом случае применение полиалфавитных кодов обеспечит вычислительным системам свойство устойчивости к отказам и сбоям.

2. Теоретические основы обнаружения и коррекции ошибок в ППМК

Известно, что для построения кодов, способных противостоять ошибкам, возникающим в комбинациях, необходимо увеличивать их избыточность. Для этого в кодовую комбинацию добавляют контрольные разряды. Как правило, для двоичных позиционных кодов эти разряды получаются путем суммирования по модулю двух соответствующих информационных разрядов [21, 22]. В результате этого для таких избыточных кодовых комбинаций наблюдается ситуация, когда информационная часть поддерживает выполнение арифметических операций, а контрольная – нет. Таким образом, при построении кодов, способных корректировать ошибки вычислений, необходимо обеспечить равноправность информационной и контрольной частей. Другими словами, с этими частями избыточной кодовой комбинации должны одинаково выполняться модульные операции.

В настоящее время теория построения корректирующих кодов системы остаточных классов достаточно глубоко проработана [9, 23, 24]. В этих кодах обнаружения и исправления ошибок в код ПСОК вводится n дополнительных контрольных модулей $m_{k+1}, m_{k+2}, \ldots, m_{k+n}$, для которых

$$m_k < m_{k+1} < \ldots < m_{k+n} \ . \tag{12}$$

В этом случае избыточная кодовая комбинация целого числа S будет иметь вид

$$S = (s_1 \ , \ s_2 \ , \ ..., \ s_k \ , \ s_{k+1}, \ ..., \ s_{k+n}) \ , \tag{13}$$

где $S \equiv s_i \ , \mathrm{mod}\, m_i ; \ i = 1, \ldots, k+n.$

При введении n контрольных модулей происходит расширение количества возможных кодовых комбинаций, которое образует полный диапазон

$$P_{пол} = \prod_{i=1}^{k+n} p_i \ = P_{\text{раб}} \prod_{i=k+1}^{k+n} p_i \ = P_{\text{раб}} P_{\text{кон}} \ . \tag{14}$$

Избыточная комбинация кода ПСОК (13) считается разрешенной, если число S принадлежит рабочему диапазону, то есть

$$S < P_{\text{раб}} \ . \tag{15}$$

Поэтому в основу большинства методов обнаружения и исправления ошибок (МОИО) положены позиционные характеристики (ПХ), которые однозначно показывают положение числа S относительно рабочего диапазона без перевода в позиционный код.

Воспользуемся этим подходом для разработки концепции построения избыточных полиалфавитных непозиционных кодов, способных обнаруживать и корректировать ошибки вычислений.

Рассмотрим код ППМК с минимальной избыточностью. Данный результат можно достичь за счет введения дополнительного контрольного остатка

$$S(x) = (s_1 \ (x), \ ..., \ s_k \ (x), \ s_{k+1}(x)) \ , \tag{16}$$

где $S(x) \equiv s_{k+1}(x) \bmod p_{k+1}(x).$

То есть необходимо добавить контрольное основание $p_{k+1}(x)$, для которого выполняется условие

$$\deg p_1 \ (x), \leq \ldots \leq \deg p_k \ (x) \leq \deg p_{k+1}(x) \ . \tag{17}$$

При введении контрольного основания произошло увеличение диапазона возможных кодовых комбинаций до полного диапазона

$$P_{пол}(x) = \prod_{i=1}^{k+1} p_i \ (x) = P_{раб}(x) p_{k+1}(x) \ . \tag{18}$$

Для избыточного ППМК комбинация (16) считается разрешенной только при условии, что

$$\deg S(x) < \deg P_{раб}(x) \ . \tag{19}$$

Ошибка вычислений приводит к искажению остатка кодовой комбинации

$$s_j^*(x) = s_j \ (x) + \Delta s_j \ (x) \ , \tag{20}$$

где + – суммирование по модулю два; $\Delta s_j(x)$ – глубина ошибки;

$$\begin{aligned} &\Delta s_j \ (x) = \left\{1, \ ..., \ x^{M_j - 1} + x^{M_j - 2} + ... + 1\right\}; \\ &M_j \ = \deg p_j \ (x). \end{aligned} \tag{21}$$

Тогда ошибочная комбинация ППМК представляется

$$S^*(x) = (s_1(x), ..., s_j^*(x), ..., s_{k+1}(x)). \quad (22)$$

Теорема 1. Если в избыточном полиалфавитном полиномиальном модулярном коде, основания которого удовлетворяют условию (18), для кодовой комбинации $S^*(x)$ не выполняется условие (19), то такая комбинация является запрещенной.

Доказательство.

Известно, что разрешенная комбинация $S(x) = (s_1(x), \ldots, s_k(x), s_{k+1}(x))$ удовлетворяет условию (20). Выполним обратный перевод из ППМК в позиционный код (ПК) с помощью Китайской теоремы об остатках в полиномах (КТОП)

$$S(x) = (s_1(x), B_1(x) + ... + s_j(x)B(x) + ... + \\ + s_{k+1}(x)B(x)) \bmod P_{\text{пол}}(x), \quad (23)$$

где $B_j(x)$ – ортогональный базис основания $p_j(x)$; $B_j(x) = m_j(x)P_{\text{пол}}(x)/p_j(x) = m_j(x)P_j(x)$; $B_j(x) \equiv 1 \bmod p_j(x)$;

$$m_j(x) = \left|P_j^{-1}(x)\right|_{p_j(x)} -$$

вес ортогонального базиса.

Пусть в комбинации $S(x)$, глубина которой равна $\Delta s_j(x) \neq 0$, произошла ошибка в j-м остатке. Тогда комбинация будет иметь вид (22). Выполним обратный перевод из ППМК в позиционный код

$$S^*(x) = \left|\sum_{\substack{i=1 \\ i \neq j}}^{k+1} s_i(x), B_i(x) + s_j^*(x)B(x)\right|_{P_{\text{пол}}(x)} = \\ = \left|\sum_{\substack{i=1 \\ i \neq j}}^{k+1} s_i(x), B_i(x) + (s_j^*(x) + \Delta s_j(x))B(x)\right|_{P_{\text{пол}}(x)} = \quad (24) \\ = S(x) + \Delta s_j(x))B_j(x).$$

Разделим комбинации $S(x)$ и $S^*(x)$ на рабочий диапазон. Если комбинация ППМК является разрешенной и выполняется условие (19), то частное от деления будет равно нулю.

$$H(x) = \left[S(x)/P_{\text{раб}}(x)\right] = 0, \quad (25)$$

где […] – целая часть числа.

Для ошибочной комбинации $S^*(x)$ получаем

$$H(x) = \left[\frac{S^*(x)}{P_{\text{раб}}(x)}\right] = \left[\frac{S(x) + \Delta s_j(x)B_j(x)}{P_{\text{раб}}(x)}\right] = \\ = \left[\frac{\Delta s_j(x)B_j(x)}{P_{\text{раб}}(x)}\right] \neq 0. \quad (26)$$

Теорема доказана.

В кодах ПСОК с помощью выражения (25) вычисляют ПХ, которая называется интервалом числа. Учитывая подобие между кодами ПСОК и ППМК, можно сделать вывод, что в качестве ПХ для последнего можно выбрать полиномиальный интервал (ПИ).

Однако введение одного контрольного остатка (основания) позволяет только обнаруживать однократные ошибки в коде. Под такими ошибками в полиалфавитных кодах понимается искажение одного остатка в комбинации. Чтобы обеспечить коррекцию такой ошибки, необходимо увеличить избыточность кода. Для этого необходимо ввести второе контрольное основание $p_{k+2}(x)$, для которого справедливо

$$\deg p_1(x), \leq ... \leq \deg p_{k+1}(x) \leq \deg p_{k+2}(x). \quad (27)$$

Докажем теорему, определяющую требования к контрольным основаниям ППМК, способным корректировать однократную ошибку.

Теорема 2. Если в избыточном полиалфавитном полиномиальном модулярном коде, для которого справедливо соотношение (27), выполняется условие

$$\deg(p_{k-1}(x)p_k(x)) \leq \deg(p_{k+1}(x)p_{k+2}(x)), \quad (28)$$

то данный код может корректировать однократную ошибку.

Доказательство. Пусть задана разрешенная кодовая комбинация, которая удовлетворяет условию (19). Введем в данную комбинацию однократную ошибку. Допустим, что в данной комбинации исказился j-й и g-й остатки, где $j \neq g$. Тогда получаем

$$S_j^*(x) = (s_1(x), ..., s_j^*(x), ..., s_{k+2}(x)), \quad (29)$$

$$S_g^*(x) = (s_1(x), ..., s_g^*(x), ..., s_{k+2}(x)), \quad (30)$$

где $s_j^*(x) = s_j(x) + \Delta s_j(x)$; $s_g^*(x) = s_g(x) + \Delta s_g(x)$.

Разделим обе комбинации на рабочий диапазон. Полученные полиномиальные интервалы должны отличаться друг от друга как минимум в одном младшем разряде. Тогда согласно (26) имеем

$$\left[\frac{S^*(x)}{P_{раб}(x)}\right] + \left[\frac{S_g^*(x)}{P_{раб}(x)}\right] \geq 1. \quad (31)$$

Согласно (26) имеем

$$\left[\frac{\Delta s_j(x)B_j(x)}{P_{раб}(x)}\right] + \left[\frac{\Delta s_g(x)B_g(x)}{P_{раб}(x)}\right] \geq 1. \quad (32)$$

Известно, что ортогональные базисы вычисляются

$$B_j(x) = \frac{m_j(x)P_{\text{пол}}(x)}{p_j(x)} = \frac{m_j(x)P_{\text{раб}}(x)P_{кон}(x)}{p_j(x)}, \quad (33)$$

$$B_g(x) = \frac{m_g(x)P_{\text{пол}}(x)}{p_g(x)} = \frac{m_g(x)P_{\text{раб}}(x)P_{кон}(x)}{p_g(x)}, \quad (34)$$

где $P_{\text{кон}}(x) = p_{k+1}(x)p_{k+2}(x)$.

Подставим (33) и (34) в выражение (32) и сократим на $P_{раб}(x)$.

$$\left[\frac{\Delta s_j(x)m_j(x)P_{\text{кон}}(x)}{p_j(x)}\right] + \left[\frac{\Delta s_g(x)m_g(x)P_{\text{кон}}(x)}{p_g(x)}\right] \geq 1. \quad (35)$$

Известно, что число полиномиальных интервалов будет равно $N_{ПИ}=2^{\deg P_{кон}(x)}$. Это позволяет перейти к вычислениям по модулю $P_{кон}(x)$. Получаем

$$P_{кон}(x)\left|\frac{\Delta s_j(x)m_j(x)}{p_j(x)}+\frac{\Delta s_g(x)m_g(x)}{p_g(x)}\right|_{P_{кон}(x)}\geq 1. \quad (36)$$

Рассмотрим второй сомножитель (36)

$$\left|\frac{\Delta s_j(x)m_j(x)p_g(x)+\Delta s_g(x)m_g(x)p_j(x)}{p_j(x)p_g(x)}\right|_{P_{кон}(x)}\geq 1. \quad (37)$$

Так как $p_j(x)$,$p_g(x)$ – неприводимые полиномы, а

$$\left|\Delta s_j(x)m_j(x)\right|_{p_j(x)}=\ddot{s}_j(x),$$

$$\left|\Delta s_g(x)m_g(x)\right|_{p_g(x)}=\ddot{s}_g(x),$$

где $\deg\ddot{s}_j(x)<\deg p_j(x)$, $\deg\ddot{s}_g(x)<\deg p_g(x)$, то

$$\left|\Delta s_j(x)m_j(x)p_g(x)+\Delta s_g(x)m_g(x)p_j(x)\right|_{P_{кон}(x)}\neq 0. \quad (38)$$

Положим, что $j=k-1$, $g=k$. В этом случае получаем

$$P_{кон}(x)\big/\left(p_{k-1}(x)p_k(x)\right)\geq 1. \quad (39)$$

Тогда справедливо,

$$\deg(p_{k-1}(x)p_k(x))\leq\deg(p_{k+1}(x)p_{k+2}(x)).$$

Теорема доказана.

3. Разработка численного метода вычисления позиционной характеристики полиномиального интервала в ППМК

В избыточных кодах ПСОК во многих МОИО используется ПХ – интервал [8]. Выбор данной позиционной характеристики определяется тем, что данная она имеет простое описание

$$H=\left[S/P_{раб}\right]. \quad (40)$$

Если выполняется условие (15), то комбинация $S=(s_1,s_2,..,s_{k+2})$ не содержит ошибки и $H=0$. Значит, она будет находиться внутри рабочего диапазона, то есть значение $H=0$. При возникновении ошибки позиция комбинации $S^*=(s_1,.s_2,..,s_{k+2})$ изменится и она будет находиться вне $P_{раб}$. В результате интервал $H\neq 0$.

Но такой подход, в котором учитывается размещение числа S относительно $P_{раб}$, нельзя использовать в полиалфавитных полиномиальных модулярных кодах. Поэтому необходимо разработать численный метод вычисления позиционной характеристики полиномиальный интервал без перевода кода ППМК в позиционный код и выполнения операции деления. Для решения данной задачи воспользуемся Китайской теоремой об остатках в полиномах, которая применяется, когда необходимо выполнить преобразование ППМК-ПК

$$S(x)=\left|\sum_{i=1}^{k+n}s_i(x),B_i(x)\right|_{P_{пол}(x)}, \quad (41)$$

где $B_j(x)$ – ортогональный базис модуля $p_j(x)$; $i=1,2,\ldots,k+n$.

Воспользуемся подобием кодов ПСОК и ППМК и вычислим полиномиальный интервал, используя выражение (41). Получаем

$$H(x)=\left[\frac{S(x)}{P_{раб}(x)}\right]=\left[\frac{\left|\sum_{i=1}^{k+n}s_i(x)B_i(x)\right|_{P_{пол}(x)}}{P_{раб}(x)}\right]. \quad (42)$$

Разделим ортогональные базисы на $P_{раб}(x)$ до получения частного $Q_i(x)$ и остатка $R_i(x)$. Тогда

$$B_i(x)=Q_i(x)P_{раб}(x)+R_i(x), \quad (43)$$

где

$$R_i(x)=\begin{cases}\tilde{B}_i(x), i=1,....,k\\ 0,\ i=k+1,...,k+n\end{cases};\ \tilde{B}_i(x)\ -$$

ортогональный базис кода с информационными основаниями.

Так как число полиномиальных интервалов равно $N_{ПИ}=2^{\deg P_{кон}(x)}$, то выражение (42) можно свести к вычислениям по модулю $P_{кон}(x)$. Тогда

$$H(x)=\left|\sum_{i=1}^{k+n}s_i(x)Q_i(x)+W(x)\right|_{P_{кон}(x)}, \quad (44)$$

где

$$W(x)=\left[\frac{\sum_{i=1}^{k}S_i(x)\tilde{B}_i(x)}{P_{раб}(x)}\right]-$$

ранг полинома при использовании информационных оснований.

Основным недостатком выражения (44) является вычисление по составному модулю $P_{кон}(x)$. Воспользуемся изоморфизмом КТОП и преобразим выражение (44) к виду

$$\begin{aligned}L_{k+1}(x)&=\left|\sum_{i=1}^{k+n}s_i(x)Q_i(x)+U(x)\right|_{p_{k+1}(x)},\\ &\vdots\\ L_{k+n}(x)&=\left|\sum_{i=1}^{k+n}s_i(x)Q_i(x)+U(x)\right|_{p_{k+n}(x)}.\end{aligned} \quad (45)$$

Анализ выражения (45) показывает, что предложенный численный метод вычисления ПХ не является оптимальным с точки зрения количества выпол-

ненных арифметических операций. Чтобы вычислить полиномиальный интервал кода ППМК, необходимо выполнить $(k+n)$ операций умножений остатков $s_i(x)$ на константы $Q_i(x)$, где $i=1,\ldots,k$, и одно сложение. Чтобы уменьшить вычислительную сложность численного метода вычисления ПХ, рассмотрим код ППМК, состоящий из k информационных оснований и одного контрольного основания $p_{k+1}(x)$. Для данного набора остатков необходимо вычислить ортогональные базисы $B_1^{k+1}(x),\ldots,B_k^{k+1}(x),B_{k+1}^{k+1}(x)$. Верхний индекс показывает, какое контрольное используется в данном избыточном коде. Полученные ортогональные базисы делятся на рабочий диапазон до получения частного $Q_i(x)$ и остатка $R_i(x)$ согласно (43). При поступлении на вход декодера избыточной комбинации ППМК с одним контрольным основанием производится вычисление полиномиального интервала по модулю $p_{k+1}(x)$.

$$L_{k+1}(x)= \\ =\left|\sum_{i=1}^{k} s_i\,(x)Q_i\,(x)+s_{k+1}(x)Q_{k+1}(x)+U(x)\right|_{p_{k+1}(x)}. \quad (46)$$

Оставим в коде ППМК k информационных основания и заменим только контрольное основание $p_{k+1}(x)$ на $p_{k+2}(x)$. Для данного набора остатков необходимо вычислить ортогональные базисы $B_1^{k+2}(x),\ldots,B_k^{k+2}(x),B_{k+1}^{k+2}(x)$. Полученные ортогональные базисы делятся на рабочий диапазон до получения остатка согласно (43). Тогда выражение (46) примет вид

$$L_{k+2}(x)= \\ =\left|\sum_{i=1}^{k} s_i(x)Q_i(x)+s_{k+2}(x)Q_{k+2}(x)+U(x)\right|_{p_{k+2}(x)}. \quad (47)$$

Реализуем данную процедуру для всех остальных контрольных оснований. Тогда численный метод вычисления ПХ кода ППМК можно представить, как

$$\begin{aligned} L_{k+1}(x)&=\left|\sum_{i=1}^{k} s_i\,(x)Q_i\,(x)+s_{k+1}(x)Q_{k+1}(x)+U(x)\right|_{p_{k+1}(x)},\\ &\vdots \\ L_{k+n}(x)&=\left|\sum_{i=1}^{k} s_i\,(x)Q_i\,(x)+s_{k+n}(x)Q_{k+n}(x)+U(x)\right|_{p_{k+n}(x)}. \end{aligned} \quad (48)$$

Анализ выражения (48) показывает, что в разработанном численном методе вычисления ПХ было сокращено количество операций умножения, что позволяет уменьшить временные затраты на коррекцию ошибочной комбинации кода ППМК. Так, при вычислении данной ПХ требуется выполнить $(k+n)$ операций умножения по модулю

$$P_{кон}(x)=\prod_{i=k+1}^{k+n} p_i\,(x).$$

А при использовании разработанного численного метода для вычисления ПХ интервальный полином требуется выполнить $(k+1)$ операцию умножения по модулю контрольного основания.

4. Результаты исследования и их обсуждение

Рассмотрим пример использования разработанного численного метода вычисления позиционной характеристики полиномиальный интервал ППМК. Пусть информационными основаниями будут $p_1(x)=x^5+x^3+x^2+x+1$, $p_2(x)=x^5+x^4+x^2+x+1$. Тогда рабочий диапазон будет равен $P_{раб}(x)=x^{10}+x^9+x^8+x^7+x^6+x^4+x^3+x^2+1$. В качестве контрольных оснований в данном коде используются два пятиразрядных неприводимых полинома. Рассмотрим первый кортеж кода ППМК с минимальной избыточностью. Пусть первым контрольным основанием будет полином $p_3(x)=x^5+x^4+x^3+x+1$. Для компактной записи используем шестнадцатеричную систему счисления. Тогда $p_3(x)=x^5+x^4+x^3+x+1=111011_2=3B_{16}$. Полный диапазон данного кода ППМК равен

$$P_{\text{пол}}^{123}(x)=x^{15}+x^{14}+x^{12}+x^8+x^7+x^6+x^5+x^4+x^3+ \\ +x^2+x+1=1101000011111111=B0FF.$$

Воспользуемся методом вычисления ортогонального базиса [5]. Для получения первого ортогонального базиса необходимо выполнить:

1. Вычислить константу

$$C_1^{123}(x)=\prod_{\substack{j=1\\ j\neq 1}}^{3} p_j(x)=10001110001=471.$$

2. Найти остаток константы по модулю $p_1(x)$

$$d_1^{123}(x)\equiv C_1^{123}(x)\bmod p_1(x)=01011=x^3+x+1.$$

3. Найти вес ортогонального базиса $m_1^{123}(x)$, для которого справедливо

$$d_1^{123}(x)m_1^{123}(x)\equiv 1\bmod p_1(x). \quad (49)$$

Получили $m_1^{123}(x)=x^4+x^3+1=11001$.

4. Вычислить ортогональный базис

$$B_1^{123}(x)=m_1^{123}(x)C_1^{123}(x)= \\ =110000011101001=60E9.$$

Аналогичным образом получаем два оставшихся ортогональных базиса

$$B_2^{123}(x)=101000101011=A2B,$$
$$B_3^{123}(x)=110101011000011=6AC3.$$

Для выполнения разработанного численного метода вычисления позиционной характеристики в ППМК представим ортогональные базисы в виде (43)

$$B_1^{123}(x)=R_1^{123}(x)P_{\text{раб}}(x)+B_1^{*}(x)= \\ =(x^4+x^2)P_{раб}(x)+(x^9+x^6+x^3+x^2+1).$$

$$B_2^{123}(x) = R_2^{123}(x)P_{раб}(x) + B_1^*(x) =$$
$$= (x+1)P_{раб}(x) + (x^9 + x^6 + x^3 + x^2).$$
$$B_3^{123}(x) = R_3^{123}(x)P_{раб}(x) = (x^4 + x^2 + x + 1)P_{раб}(x).$$

Тогда имеем

$$Q_1^{123}(x) = x^4 + x^2 = 10100.$$
$$Q_2^{123}(x) = x + 1 = 00011.$$
$$Q_1^{123}(x) = x^4 + x^2 + x + 1 = 10111.$$

Данные значения будут использоваться при вычислении значения полиномиального интервала по модулю $p_3(x) = x^5 + x^4 + x^3 + x + 1$.

Рассмотрим второй кортеж кода ППМК. В качестве второго контрольного основания выбираем $p_4(x) = x^5 + x^2 + 1$. Тогда код ППМК имеет $p_1(x) = x^5 + x^3 + x^2 + x + 1$, $p_2(x) = x^5 + x^4 + x^2 + x + 1$, а информационные основания и контрольное основание $p_4(x) = x^5 + x^2 + 1$. Тогда полный диапазон равен

$$P_3(x) = x^{15} + x^{14} + x^{13} + x^9 + x^8 + x^3 + 1 =$$
$$= 1110001100001001 = E309.$$

Произведем вычисление первого ортогонального базиса для данного кортежа оснований. Для получения первого ортогонального базиса необходимо выполнить:

1. Вычислить константу

$$C_1^{124}(x) = p_2(x)p_4(x) = 110000001011 = 70D.$$

2. Найти остаток константы по модулю $p_1(x)$

$$d_1^{124}(x) \equiv C_1^{124}(x) \bmod p_1(x) = 10010 = x^4 + x.$$

3. Найти вес ортогонального базиса $m_1^{124}(x)$, для которого справедливо

$$d_1^{124}(x)m_1^{143}(x) \equiv 1 \bmod p_1(x).$$

Получили $m_1^{124}(x) = x^4 + x^3 + x^2 + 1 = 11101$.

4. Вычислить ортогональный базис

$$B_1^{124}(x) = m_1^{124}(x)C_1^{124}(x) = 100111011001111 = 4ECF.$$

Аналогичным образом получаем другие ортогональные базисы

$$B_2^{124}(x) = 10010000001101 = 240D,$$
$$B_3^{124}(x) = 110101011000011 = 6AC3.$$

Воспользуемся выражением (43) и представим ортогональные базисы в виде

$$B_1^{124}(x) = R_1^{124}(x)P_{раб}(x) + B_1^*(x) =$$
$$= (x^4 + x^3 + x)P_{раб}(x) + (x^9 + x^6 + x^3 + x^2 + 1).$$
$$B_2^{124}(x) = R_2^{124}(x)P_{раб}(x) + B_1^*(x) =$$
$$= (x^3 + x^2 + 1)P_{раб}(x) + (x^9 + x^6 + x^3 + x^2).$$
$$B_2^{124}(x) = R_3^{124}(x)P_{раб}(x) = (x^4 + x^2 + x + 1)P_{раб}(x).$$

Тогда имеем

$$Q_1^{124}(x) = x^4 + x^2 + x = 10110.$$
$$Q_2^{124}(x) = x^3 + x^2 + 1 = 01101.$$
$$Q_3^{124}(x) = x^4 + x^2 + x + 1 = 10111.$$

Выберем в качестве полинома $S(x) = x^7$, который удовлетворяет условию (19). Представим полином в коде ППМК с двумя контрольными основаниями

$$S(x) = (x^4 + x + 1, x^2 + 1, x^4 + x^3 + x, x^4 + x^2).$$

Для обнаружения и коррекции ошибки в ППМК сначала используем первый кортеж, состоящий из $p_1(x) = x^5 + x^3 + x^2 + x + 1$, $p_2(x) = x^5 + x^4 + x^2 + x + 1$, $p_3(x) = x^5 + x^4 + x^3 + x + 1$ оснований. Тогда имеем комбинацию

$$S(x) = (x^4 + x + 1, x^2 + 1, x^4 + x^3 + x) =$$
$$= (10011, 00101, 11010).$$

Вычислим ранг полинома при использовании информационных оснований. Получаем

$$W(x) = \left[\frac{(x^4 + x + 1)B_1^* + (x^2 + 1)B_2^*}{x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1} \right] =$$
$$= x^3 + x^2 + x + 1.$$

Вычислим значение полиномиального интервала, представленного по первому контрольному основанию, используя выражение (46). Представим аргументы выражения (46) в виде элементов поля Галуа GF(2^5), порожденных $p_3(x) = x^5 + x^4 + x^3 + x + 1$.

$$s_1(x) = 10011 = \beta^{29}, s_2(x) = 00101 = \beta^{13},$$
$$s_3(x) = 11010 = \beta^7, W(x) = 01111 = \beta^8,$$
$$Q_1^{123}(x) = x^4 + x^2 = 10100 = \beta^9,$$
$$Q_2^{123}(x) = x^2 + 1 = 00101 = \beta^8,$$
$$Q_1^{123}(x) = x^4 + x^2 + x + 1 = 10111 = \beta^{26}.$$

Тогда

$$L_3(x) = \left| \sum_{i=1}^{2} s_i(x)Q_i(x) + s_3(x)Q_3(x) + U(x) \right|_{p_3(x)} =$$
$$= \left| \beta^{29} \cdot \beta^{28} + \beta^{26} \cdot \beta^{13} + \beta^7 \cdot \beta^{19} + \beta^8 \right|_{x^4 + x^3 + x + 1} = 0.$$

Представим заданный полином в коде ППМК, используя второй кортеж, состоящий из оснований $p_1(x) = x^5 + x^3 + x^2 + x + 1$, $p_2(x) = x^5 + x^4 + x^2 + x + 1$, $p_3(x) = x^5 + x^2 + 1$. Тогда имеем комбинацию

$$S(x) = (x^4 + x + 1, x^2 + 1, x^4 + x^2) =$$
$$= (10011, 00101, 10100).$$

Вычислим значение полиномиального интервала, представленного по второму контрольному основанию, используя выражение (46). Представим аргу-

менты выражения (46) в виде элементов поля Галуа GF(2^5), порожденных $p_3(x)=x^5+x^2+1$.

$$s_1(x)=10011=\beta^{17}, s_2(x)=00101=\beta^5,$$
$$s_3(x)=10100=\beta^7, W(x)=01111=\beta^{23},$$
$$Q_1^{124}(x)=x^4+x^2+x=10110=\beta^9,$$
$$Q_2^{124}(x)=x^3+x^2+1=01101=\beta^8$$
$$Q_3^{124}(x)=x^4+x^2+x+1=10111=\beta^{26}.$$

Тогда

$$L_4(x)=\left|\sum_{i=1}^{2} s_i(x)Q_i(x)+s_4(x)Q_4(x)+U(x)\right|_{p_4(x)}=$$
$$=\left|\beta^{17}\cdot\beta^9+\beta^5\cdot\beta^8+\beta^7\cdot\beta^{26}+\beta^{23}\right|_{x^4+x^2+1}=0.$$

Так как значение полиномиального интервала равно $L_3(x)=L_4(x)=0$, то комбинация

$$S(x)=(x^4+x+1, x^2+1, x^4+x^3+x, x^4+x^2)$$

не содержит ошибки.

Пусть ошибка возникла в первом остатке, а ее глубина равна $\Delta s_1(x)=1$. Тогда искаженный остаток

$$s_1^*(x)=s_1(x)+\Delta s_1(\mathrm{x})=\mathrm{x}^4+x\ .$$

В результате этого ошибочная комбинация кода ППМК примет вид

$$S(x)=(x^4+x, x^2+1, x^4+x^3+x, x^4+x^2)\ .$$

Воспользуемся разработанным численным методом вычисления ПХ. Для обнаружения и коррекции ошибки в ППМК сначала используем первый кортеж, состоящий из $p_1(x)=x^5+x^3+x^2+x+1$, $p_2(x)=x^5+x^4+x^2+x+1$, $p_3(x)=x^5+x^4+x^3+x+1$ оснований. Тогда имеем комбинацию

$$S^*(x)=(x^4+x, x^2+1, x^4+x^3+x)=(10010, 00101, 11010).$$

Вычислим ранг полинома при использовании информационных оснований. Получаем

$$W(x)=\left[\frac{(x^4+x+1)B_1^*+(x^2+1)B_2^*}{x^{10}+x^9+x^8+x^7+x^6+x^4+x^3+x^2+1}\right]=$$
$$=x^3+x^2+x+1.$$

Представим аргументы выражения (46) в виде элементов поля Галуа GF(2^5), порожденных $p_3(x)=x^5+x^4+x^3+x+1$.

$$s_1(x)=10010=\beta^{24}, s_2(x)=00101=\beta^{13},$$
$$s_3(x)=11010=\beta^7, W(x)=01111=\beta^8.$$

Тогда

$$L_3(x)=\left|\sum_{i=1}^{2} s_i(x)Q_i(x)+s_3(x)Q_3(x)+U(x)\right|_{p_3(x)}=$$
$$=\left|\beta^{24}\cdot\beta^{28}+\beta^{26}\cdot\beta^{13}+\beta^7\cdot\beta^{19}+\beta^8\right|_{x^4+x^3+x+1}=01110.$$

Представим аргументы выражения (46) в виде элементов поля Галуа GF(2^5), порожденных $p_3(x)=x^5+x^2+1$.

$$s_1(x)=10010=\beta^{30}, s_2(x)=00101=\beta^5,$$
$$s_3(x)=10100=\beta^7, W(x)=01111=\beta^{23}.$$

Тогда

$$L_4(x)=\left|\sum_{i=1}^{2} s_i(x)Q_i(x)+s_4(x)Q_4(x)+U(x)\right|_{p_4(x)}=$$
$$=\left|\beta^{30}\cdot\beta^9+\beta^5\cdot\beta^8+\beta^7\cdot\beta^{26}+\beta^{23}\right|_{x^4+x^2+1}=11010.$$

В результате получили, что позиционная характеристика отлична от нуля, что свидетельствует о том, что комбинация ППМК содержит ошибку. Значению ПХ $L_3(x)=11010$, $L_4(x)=11010$ соответствует вектор ошибки

$$\overline{e}=(00001, 00000, 00000, 00000, 00000).$$

Чтобы исправить ошибку, необходимо к искаженной комбинации прибавить вектор ошибки.

$$S(x)=S^*(x)+\overline{e}=(x^4+x, x^2+1, x^4+x^3+x)+$$
$$+(00001, 00000, 00000, 00000, 00000)=$$
$$=(10011, 00101, 11010).$$

Используя разработанный численный метод вычисления ПХ полиномиальный, ошибка в коде ППМК была обнаружена и исправлена.

Заключение

В статье рассмотрены основные принципы построения полиалфавитных полиномиальных модулярных кодов. Показано, что благодаря распараллеливанию таких арифметических операций, как сложение, вычитание и умножение, применение кодов ППМК позволяет повысить производительность вычислительных систем. При этом коды ППМК обладают потенциальными возможностями по обнаружению и коррекции ошибок, возникающих в процессе вычислений. Это обусловлено равноправностью и независимостью оснований ППМК. В статье представлены теоретические основы построения избыточных ППМК, способных обнаруживать и корректировать ошибки вычислений. На основе доказанных теорем был разработан численный метод вычисления позиционной характеристики полиномиальный интервал в ППМК, который требует меньших временных затрат. Так, при вычислении данной ПХ на основе Китайской теоремы об остатках в полиномах требовалось выполнить (k+n) операций умножения по модулю

$$P_{кон}(x)=\prod_{i=k+1}^{k+n} p_i(x),$$

а при использовании разработанного численного метода для вычисления ПХ требуется выполнить (k+1)

операцию умножения по модулю контрольного основания. Представленный в статье пример подтвердил выводы.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования в рамках работ Российского научного фонда (проект №23-21-00036, https://rscf.ru/project/23-21-00036/).

References

[1] Svoboda A. Rational numerical system of residual classes. In Book: Svoboda A, ed. Stroje na Zpracování Informací. Sborník V. Praha: Československá akademie věd; 1957: 9-37.
[2] Akushsky IYa, Yuditsky DI. Machine arithmetic in residual classes [In Russian]. Moscow: "Sovetskoe Radio" Publisher; 1968.
[3] Amerbaev VM, Pak IT. Parallel computing in the complex plane [In Russian]. Alma-Ata: "Nauka" Publisher; 1984.
[4] Amerbaev VM, Biyashev RG, Vilansky YuV. Cryptographic methods of information protection [In Russian]. Moscow: "Radiotehnika" Publisher; 2007. ISBN: 5-88070-131-X.
[5] Torgashev VA. The system of residual classes and the reliability of digital computers [In Russian]. Moscow: "Sovetskoe Radio" Publisher; 1973.
[6] Ananda M. Residue number systems. Theory and applications. Switzerland: Springer International Publishing; 2016. ISBN: 978-3-319-41385-3.
[7] Finko OA, Kuzmenko AS, Lisitsyn VV. Algorithm for operating a computational channel by an arbitrary module based on the implementation of arithmetical operations by numerical polynomials. Information security is a pressing problem of our time. Improving educational technologies for training specialists in the field of information security 2018: 1(9): 142-147.
[8] Chervyakov NI, Shaposhnikov AV, Sakhnyuk PA, Makokha AN, eds. Neurocomputers in residual classes [In Russian]. Moscow: "Radiotehnika" Publisher; 2003. ISBN: 5-93108-054-6.
[9] Omondi A, Premkumar B. Residue number systems: Theory and implementation. London, UK: Imperial College Press; 2007. ISBN: 978-1-86094-866-4.
[10] Chang CH, Molahosseini AS, Zarandi AAE, Tay TF. Residue number systems: a new paradigm to datapath optimization for low-power and high-performance digital signal processing applications. IEEE Circuits Syst Mag 2015; 15(4): 26-44. DOI: 10.1109/MCAS.2015.2484118.
[11] Jyothi GN, Sanapala K, Vijayalakshmi A. ASIC implementation of distributed arithmetic based FIR filter using RNS for high speed DSP systems. Int J Speech Technol 2020; 23: 259-264. DOI: 10.1007/s10772-020-09683-1.
[12] Murthy SC, 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.
[13] Balaji M, Padmaja N. Area and delay efficient RNS-based FIR filter design using fast multipliers. Meas: Sens 2024; 31: 101014. DOI: 10.1016/j.measen.2023.101014.
[14] Valueva MV, Lyakhov PA, Nagornov NN, Valuev GV. High-performance digital image filtering architectures in the residue number system based on the Winograd method. Computer Optics 2022; 46(5): 752-762. DOI: 10.18287/2412-6179-CO-933.
[15] Lyakhov PA, Nagornov NN, Semyonova NF, Abdulsalyamova AS. Development of digital image processing algorithms based on the Winograd method in general form and analysis of their computational complexity. Computer Optics 2023; 47(1): 68-78. DOI: 10.18287/2412-6179-CO-1146.
[16] Kalmylov IA, Kopytov VV, Olenev AA. Application of modular residue classes codes in an authentication protocol for satellite internet systems. IEEE Access 2023; 11: 71624-71633. DOI: 10.1109/ACCESS.2023.3290498.
[17] Olenev AA, Kalmykov IA, Pashintsev VP. Improved spacecraft authentication method for satellite internet system using residue codes. Information 2023; 14(7): 407. DOI: 10.3390/info14070407.
[18] Chervyakov NI, Evdokimov AA, Galushkin AI, Lavrinenko IN. Application of artificial neural networks and residual class systems in cryptography [In Russian]. Moscow: "Fizmatlit" Publisher; 2012. ISBN: 978-5-9221-1386-1.
[19] Prabhashana S, Sajan S, Sajan P. Modelling of parallel unsigned 2n–1 modular arithmetic multiplier for RNS. March 2021. IOP Conf Ser Mater Sci Eng 2021: 1084(1): 012060. DOI: 10.1088/1757-899X/1084/1/012060.
[20] Elango S, Sampath P, Raja Sekar S, Philip SP, Danielraj A. High-performance multi-RNS-assisted concurrent RSA cryptosystem architectures. J Circuit Syst Comp 2023: 32(15): 2350255. DOI: 10.1142/S0218126623502559.
[21] Kudryashov BD. Fundamentals of coding theory [In Russian]. Saint-Petersburg: "BHV-Petersburg" Publisher; 2012. ISBN: 978-5-9775-3527-4.
[22] Sidelnikov VM. Coding theory [In Russian]. Moscow: "Fizmatlit" Publisher; 2008. ISBN: 978-5-9221-0943-7.
[23] Chervyakov NI, Kolyada AA, Lyakhov PA Modular arithmetic and its applications in infocommunication technologies [In Russian]. Moscow: "Fizmatlit" Publisher; 2017. ISBN: 978-5-9221-1716-6
[24] Molahosseini AS, de Sousa LS, Chang C-H, eds. Embedded systems design with special arithmetic and number systems. Cham, Switzerland: Springer International Publishing AG; 2017. ISBN: 978-3-319-49741-9.

Сведения об авторах

Калмыков Игорь Анатольевич, доктор технических наук, профессор кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета. Область научных интересов: непозиционные системы счисления, параллельные вычисления, отказоустойчивые вычислительные системы. E-mail: *kia762@yandex.ru*

Оленев Александр Анатольевич, кандидат технических наук, старший научный сотрудник Института цифрового развития Северо-Кавказского федерального университета. Область научных интересов: непозиционные системы счисления, отказоустойчивые вычислительные системы, математическая логика.
E-mail: *olenevalexandr@gmail.com*

Кононова Наталья Владимировна, кандидат физико-математических наук, заведующая кафедрой информационной безопасности автоматизированных систем Северо-Кавказского федерального университета. Область научных интересов: математическое моделирование сложных систем, криптографические методы защиты информации, модульная арифметика. E-mail: *knv_fm@mail.ru*

Пелешенко Татьяна Александровна, кандидат технических наук, доцент кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета. Область научных интересов: непозиционные системы счисления, методы и алгоритмы вейвлет-анализа для цифровой обработки сигналов. E-mail: *gtanya09@mail.ru*

Чистоусов Никита Константинович, кандидат технических наук, старший научный сотрудник Института цифрового развития Северо-Кавказского федерального университета. Область научных интересов: криптографические методы защиты информации, протоколы аутентификации с нулевым разглашением, непозиционные системы счисления. E-mail: *chistousov.nik@yandex.ru*

ГРНТИ: 28.21.19
Поступила в редакцию 13 февраля 2024 г. Окончательный вариант – 12 апреля 2024 г.

A numerical method for parallel calculation of the positional characteristic for error correction in a polyalphabetic polynomial modular code

I.A. Kalmykov [1], A.A. Olenev [1], N.V. Kononova [1], T.A. Peleshenko [1], N.K. Chistousov [1]
[1] North Caucasus Federal University, 355017, Stavropol, Russia, Pushkin Str, 1

Abstract

The trend toward increasing the efficiency of computing systems and devices is directly related with the transition to parallel computing. We propose that parallel calculations should be conducted at the level of arithmetic operations using arithmetic composite modular codes (CMC), in which code combinations represent a set of residues obtained by dividing an integer into bases. There are two types of such codes. In the polyalphabetic code of the residual number system (PCRNS), mutually prime numbers are used as bases. In polyalphabetic polynomial modular code (PPMC) there are irreducible polynomials. A characteristic feature of these codes is that addition, subtraction and multiplication operations are implemented in parallel in bases. There is no data exchange between the bases. As a result, an increase in the productivity of computing systems is achieved. The bases of polyalphabetic modular codes are equal, independent, and serve as a basis for constructing arithmetic codes that detect and correct errors that occur in the calculation process. The article presents theoretical foundations for constructing a redundant PPMC capable of detecting and correcting computational errors. On the basis of the proved theorems, a numerical method for calculating the positional characteristic (PH) of the polynomial interval in PPMC was developed. This method requires fewer multiplication operations compared to the classical method of calculating this PH. Examples of the application of this method are considered.

Keywords: parallel calculations, polyalphabetic polynomial modular code, control bases, numerical method for calculating positional characteristics, error correction.

Citation: 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.

Acknowledgements: This work was financially supported by the Russian Science Foundation under project No. 23-21-00036 (https://rscf.ru/project/23-21-00036).

Authors' information

Igor Anatolyevich Kalmykov, Doctor of Technical Sciences, Professor of Information Security of Automated Systems department of the North Caucasus Federal University. The field of scientific interests: non-positional number systems, parallel computing, fault-tolerant computing systems. E-mail: *kia762@yandex.ru*

Alexander Anatolyevich Olenev, Candidate of Technical Sciences, Senior Researcher at the Institute of Digital Development of the North Caucasus Federal University. Research interests: non-positional number systems, fault-tolerant computing systems, mathematical logic. E-mail: *olenevalexandr@gmail.com*

Natalia Vladimirovna Kononova, Candidate of Physical and Mathematical Sciences, Head of Information Security of Automated Systems department of the North Caucasus Federal University. Research interests: mathematical modeling of complex systems, cryptographic methods of information protection, modular arithmetic.
E-mail: *knv_fm@mail.ru*

Tatyana Alexandrovna Peleshenko, Candidate of Technical Sciences, Associate Professor of Information Security of Automated Systems department of the North Caucasus Federal University. Research interests include non-positional number systems, methods and algorithms of wavelet analysis for digital signal processing.
E-mail: *gtanya09@mail.ru*

Nikita Konstantinovich Chistousov, Candidate of Technical Sciences, Senior Researcher at the Institute of Digital Development of the North Caucasus Federal University. Research interests: cryptographic methods of information protection, zero-knowledge authentication protocols, non-positional number systems.
E-mail: *chistousov.nik@yandex.ru*

Received February 13, 2024. The final version – April 12, 2024.