DOI: 10.15514/ISPRAS-2024-36(1)-5

Применение энтропии для обнаружения ошибок модулярного кода в системах надежного распределенного хранения

[1,2] *В.А. Кучуков, ORCID: 0000-0002-1839-2765 <vkuchukov@ncfu.ru>*

[1] *Северо-Кавказский центр математических исследований,*
Северо-Кавказский федеральный университет,
355017, Россия, г. Ставрополь, ул. Пушкина, 1.
[2] *Институт системного программирования РАН им. В.П. Иванникова,*
109004, Россия, г. Москва, ул. А. Солженицына, д. 25.

Аннотация. В статье рассмотрена проблема обнаружения и локализации ошибок модулярного кода. Рассмотрено применение энтропии для обнаружения ошибок полиномиальной системы классов вычетов, исправление ошибок в которой осуществляется методом наибольшего правдоподобия. Для системы остаточных классов предложен подход к обнаружению ошибок через энтропию, позволяющий обнаружить ошибки большей кратности, по сравнению с классическим подходом. Для исправления ошибок рассмотрены методы наибольшего правдоподобия и метод проекций. Введенные ограничения на избыточное основание СОК позволило обнаружить не только все одиночные ошибки по рабочим модулям, но также и ряд ошибок по двум основаниям. Предложена система надежного распределенного хранения, позволяющая обнаружить и исправить ошибки, возникающие при приеме данных из облаков.

Ключевые слова: система остаточных классов; полиномиальная система классов вычетов; энтропия; обнаружение ошибок.

Для цитирования: Кучуков В.А. Применение энтропии для обнаружения ошибок модулярного кода в системах надежного распределенного хранения. Труды ИСП РАН, том 36, вып. 1, 2024 г., стр. 61–72. DOI: 10.15514/ISPRAS–2024–36(1)–5.

Благодарности: Работа выполнена при поддержке Российского научного фонда 19-71-10033, https://rscf.ru/project/19-71-10033/.

Application of Entropy for Modular Code Error Detection in Reliable Distributed Storage Systems

[1,2] *V.A. Kuchukov ORCID: 0000-0002-1839-2765 <vkuchukov@ncfu.ru>*

[1] *North-Caucasus Center for Mathematical Research, North-Caucasus Federal University,*
1, Pushkin st., Stavropol, 355017, Russia.
[2] *Ivannikov Institute for System Programming of the Russian Academy of Sciences,*
25, Alexander Solzhenitsyn st., Moscow, 109004, Russia.

Abstract. The paper considers the problem of error detection and localization of modular code. The polynomial residue number system represents the input number as a set of polynomials over the finite field GF(2^m), which are residues from dividing the original polynomial by a set of irreducible polynomials. The introduction of redundant moduli provides the required corrective capability of the noise-tolerant code. The application of entropy for error detection of a polynomial residue number system, error correction of which is performed by

the maximum likelihood method, is considered. In the residue number system, a number is represented as residues from division by a set of mutually prime numbers. An approach to error detection through entropy is proposed for the residue number system, which allows to detect errors of higher multiplicity compared to the classical approach. The maximum likelihood and projection methods are considered for error correction. The introduced constraints on the control modulo allowed us to detect not only all single errors on working moduli, but also a number of errors on two moduli. A computational experiment was carried out to investigate the corrective abilities for three sets of moduli {3, 5, 7, 8}, {3, 5, 7, 37}, {3, 5, 7, 71}. A reliable distributed storage system is proposed to detect and correct errors that occur when data is ingested from clouds.

Keywords: residue number system; polynomial residue number system; entropy; error detection.

For citation: Kuchukov V.A. Application of entropy for modular code error detection in reliable distributed storage systems. *Trudy ISP RAN/Proc. ISP RAS*, vol. 36, issue 1, 2024. pp. 61-72 (in Russian). DOI: 10.15514/ISPRAS-2024-36(1)-5.

Acknowledgements. This work was supported by the Russian Science Foundation 19-71-10033, https://rscf.ru/project/19-71-10033/.

1. Введение

Для многих удаленных инфраструктурных объектов, таких как системы контроля на железной дороге или нефтеперерабатывающей промышленности, важно обеспечение надежной работы и гарантированной достоверности получаемых результатов. При этом для каналов связи вероятность однократных ошибок значительно выше вероятности ошибок большей кратности [1-2]. Таким образом, актуальной является проблема использования корректирующих кодов, позволяющих обнаружить и исправить одиночную ошибку. При этом использование корректирующих кодов связано с проблемой, что зачастую информация в них строго делится на информационную и контрольную, при этом контрольные цифры числа не позволяют производить вычисления над избыточными числами [3]. К кодам, в которых информационная и контрольная части числа равноценны, относятся полиномиальная система классов вычетов и система остаточных классов. Для обеспечения возможности определения ошибок рассмотрим понятие энтропии.

Рассмотрим подход к определению «количества информации», рассмотренный в статье [4]. Если в некотором множестве X, состоящем из N элементов, задана переменная x, то энтропия переменной x равна

$$H(x) = \log_2 N.$$

При этом для передачи количества информации I необходимо употреблять $\lceil \log_2 N \rceil$ двоичных символов. Например, для кодирования в двоичной системе счисления чисел от 0 до 5 необходимо $\lceil \log_2 6 \rceil = 3$ двоичных знака.

Если переменные $x_1, x_2, \dots, x_n$ принимают значения из множеств, состоящих из $N_1, N_2, \dots, N_n$ элементов соответственно, то

$$H(x_1, x_2, \dots, x_n) = H(x_1) + H(x_2) + \cdots + H(x_k).$$

Рассмотрим применение данного понятия для обнаружения и исправления ошибок полиномиальной системой классов вычетов и системой остаточных классов.

Далее статья организована следующим образом. В разделе 2 рассмотрена полиномиальная система классов вычетов с возможностью обнаружения и коррекции ошибки на основе энтропии и метода наибольшего правдоподобия. В разделе 3 рассмотрены корректирующие свойства избыточной системы остаточных классов. В разделе 4 рассмотрен вычислительный эксперимент, описывающий особенности обнаружения и исправления ошибок с избыточным модулем специального вида. В разделе 5 рассмотрена модель системы надежного распределенного хранения в системе остаточных классов. В заключении обобщены полученные результаты и даны рекомендации по использованию корректирующих модулярных кодов.

2. Корректирующие свойства полиномиальной системы классов вычетов

Одним из способов обеспечения надежности при хранении информации в облаках является использование при разделении данных схем разделения секрета (СРС), в частности взвешенных СРС [5], в которых данные делятся на доли разного размера, зависящего от надежности хранилища. Исходные данные могут быть восстановлены в случае некорректности одной или нескольких долей.

В качестве схемы разделения секрета может быть взята избыточная полиномиальная система классов вычетов (ПСКВ, PRNS). Возьмем исходные данные A, которые могут быть представлены в виде многочлена $A_P(x)$ над полем $GF(2^m)$ в виде $A_P(x) = \sum_{i=1}^{m-1} f_i \cdot x^i$, где $f_i \in \{0,1\}$ [5].

Избыточная ПСКВ представляет собой набор из n неприводимых многочленов $m_1(x), m_2(x), \ldots, m_n(x)$, где n – общее количество модулей ПСКВ, r – количество избыточных модулей ПСКВ, тогда $k = n - r$ – количество рабочих модулей, при этом d_i – степень многочлена $m_i(x)$. Тогда любой многочлен $A_P(x)$ представляется в виде остатков от деления на модули ПСКВ, т.е. $A_{PRNS} = \big(a_1(x), a_2(x), \ldots, a_n(x)\big)$. При этом $M(x) = \prod_{i=1}^{k} m_i(x)$ – рабочий диапазон $\big[0, M(x)\big)$ со степенью $D = \deg M(x) = \sum_{i=1}^{k} d_i$, а $\widehat{M}(x) = \prod_{i=1}^{n} m_i(x)$ – полный диапазон $\left[0, \widehat{M}(x)\right)$ со степенью $\widehat{D} = \deg \widehat{M}(x) = \sum_{i=1}^{n} d_i$. Если $\deg A_P(x) < D$, то представление $A_P(x)$ единственное.

За счет вводимых избыточных модулей может быть проведено определение ошибки вычисления или передачи данных. Если полученный при восстановлении многочлен удовлетворяет выражению $\deg A_P(x) < D$, то многочлен корректен или содержит более сложную комбинацию ошибок, чем способен распознать избыточный код, если же $\deg A_P(x) \geq D$, то многочлен содержит ошибку. Таким образом, ошибка может быть обнаружена, если многочлен имеет степень большую, либо равную D, но меньшую $\widehat{D}$.

Одним из подходов к восстановлению многочлена из его представления в виде остатков является вариант Китайской теоремы об остатках для многочленов, а именно

$$A_P(x) = \left| \sum_{i=1}^{n} a_i(x) \cdot \left|\widehat{M}_i^{-1}(x)\right|_{m_i(x)} \cdot \widehat{M}_i(x) \right|_{\widehat{M}(x)},$$

где $\widehat{M}_i(x) = \widehat{M}(x)/m_i(x)$ и $\left|\widehat{M}_i^{-1}(x)\right|_{m_i(x)}$ – мультипликативные инверсии, для которых выполняется $\left|\widehat{M}_i^{-1}(x)\right|_{m_i(x)} \cdot \widehat{M}_i(x) \bmod m_i(x) = 1$.

Рассмотрим вопрос избыточности данных. Многочлен, входящий в рабочий диапазон, имеет степень, меньшую D, таким образом можно сказать, что на представление исходного числа требуется D бит. С учетом избыточных модулей степень многочлена в избыточной ПСКВ ограничена $\widehat{D}$. Тогда в случае сбалансированной системы все остатки используют $d_1 = d_2 = \cdots = d_n = d$ бит и избыточность равна

$$R = \frac{\widehat{D}}{D} - 1 = \frac{n \cdot d}{k \cdot d} - 1 = \frac{n-k}{k}.$$

Многочлен, содержащий ошибку может быть представлен в виде $\overline{A}_{PRNS} = A_{PRNS} + E_{PRNS}$, при этом ошибка имеет форму $E(x) = \beta(x)\widehat{M}_I(x)$, где $\beta(x)$ – ненулевой многочлен, $\widehat{M}_I(x) = \prod_{i \in I} m_i(x)$ и I – множество остатков без ошибки [5].

В статье [5] также введено понятие энтропии для полиномиальной системы классов вычетов. Поскольку степень $A_P(x)$ меньше D, то $A_P(x)$ может принимать 2^D различных значения. Тогда, согласно [4], энтропия $A_P(x)$ будет равна

$$H\big(A_P(x)\big) = \log_2 2^D = D = \sum_{i=1}^{k} d_i.$$

Если $i \in [1,n]$ и $a_i(x) = |A_P(x)|_{m_i(x)}$, то энтропия $a_i(x)$ равна d_i:

$$H\big(a_i(x)\big) = d_i.$$

Таким образом, остатки $a_i(x)$ содержат некоторую информацию об $A_P(x)$. Если $H\big(a_i(x)\big) = 0$, то остаток не содержит информации о $A_P(x)$, если же энтропия равна D, то имеется полная информация о $A_P(x)$. Если количество известной информации больше или равно исходной, то выполняется выражение

$$\sum_{i\in I} d_i \geq \sum_{i=1}^{k} d_i.$$

Таким образом, мы можем безошибочно восстановить $A_P(x)$.

В [5] приведена следующая теорема об обнаружении ошибки.

Теорема 1. Если задана полиномиальная система классов вычетов с n модулями $m_1(x)$, $m_2(x)$, …, $m_n(x)$, где r – количество избыточных модулей, и $k = n - r$ – количество рабочих модулей, то для многочлена $A_P(x)$, представленного в виде остатков $\overline{A}_{PRNS} = \big(\overline{a}_1(x), \overline{a}_2(x), \dots, \overline{a}_n(x)\big)$ и множества $\overline{I}$ остатков с ошибкой, ошибка может быть обнаружена, если выполняется условие

$$\sum_{i\in\overline{I}} d_i \leq \sum_{i=1}^{r} d_{k+i}.$$

Таким образом, для обнаружения ошибки используется Теорема 1. Для локализации и исправления ошибки в статье [5] модифицирован метод декодирования с максимальным правдоподобием (MLD) [6]. Для исправления ошибки множество остатков без ошибок должно удовлетворять условию $\sum_{i\in I} d_i > D$. В процессе локализации и исправления ошибок находится множество V возможных кандидатов $A_P(x)$, удовлетворяющих условию $\deg A_P\,(x) < D$. Каждый из возможных $A_P(x)$ обозначается $V_P^l(x)$, т.е:

$$V = \big\{V_P^1(x), V_P^2(x), \dots, V_P^\lambda(x)\big\},$$

где λ – количество кандидатов, попадающих в разрешенный диапазон.

Поскольку в общем случае ПСКВ относится к взвешенным кодам коррекции ошибок, для которых $d_1 \neq d_2 \neq \cdots \neq d_n$, то расстояние Хэмминга H_T^l, которое определяется как количество элементов, по которым различаются два вектора V_{PRNS}^l и $\overline{A}_{PRNS}$, не обеспечивает корректной оценки, поскольку остатки несут разное количество информации об $A_P(x)$.

Для вычисления веса Хэмминга H_W^l кандидата $V_{PRNS} = \big(v_1(x), v_2(x), \dots, v_n(x)\big)$ в случае получения значения с ошибкой $\overline{A}_{PRNS} = \big(\overline{a}_1(x), \overline{a}_2(x), \dots, \overline{a}_n(x)\big)$ в статье [5] предложен алгоритм согласно которому вычисление H_W^l проходит в три этапа: на первом этапе вычисляется вектор Хэмминга $h = (h_1, h_2, \dots, h_n)$, где $h_i = 0$ когда $v_i(x) = \overline{a}_i(x)$, иначе $h_i = 1$. На втором шаге вычисляется обратная величина вектора h, $\overline{h} = \big(\overline{h}_1, \overline{h}_2, \dots, \overline{h}_n\big)$, где $\overline{h}_i$ равно единице, если остаток $a_i(x)$ не содержит ошибки, в противном случае $\overline{h}_i$ равно нулю. Третьим шагом является вычисление величины энтропии H_W^l как поэлементное произведение двух векторов: $\overline{h} = \big(\overline{h}_1, \overline{h}_2, \dots, \overline{h}_n\big)$ и вектора, состоящего из энтропий остатков от деления, $\overline{a}_i(x)$, т.е. $H_W^l = \overline{h} \cdot h_E$, где $h_E = \Big(H\big(\overline{a}_1(x)\big), H\big(\overline{a}_2(x)\big), \dots, H\big(\overline{a}_n(x)\big)\Big) = (d_1, d_2, \dots, d_n)$.

Пример 1. Рассмотрим к качестве полиномиальной системы классов вычетов набор модулей $\{x^2+x+1, x^3+x+1, x^3+x^2+1, x^6+x+1\}$ для которого $h_E=(2,3,3,6)$, рабочий диапазон $M(x)=x^8+x^6+x^5+x^4+x^3+x^2+1$, полный диапазон $\widehat{M}=x^{14}+x^{12}+x^{11}+x^{10}+x^7+x^6+x^2+x+1$. Избыточность данной системы равна $R=\widehat{D}/D-1=14/8-1=3/4$. В статье [5] в примере 4 указано, что кандидаты должны удовлетворять условию $\deg V_P^l(x)<D=\sum_{i=1}^{k} d_i$.

Введем в многочлен $A(x)=x^7+x^5+x^3+x+1=(x+1, x^2+x, x^2, x^5+x^3+x^2+1)$ ошибку по второму модулю $E=(0,1,0,0)$, получим многочлен $\overline{A}_{PRNS}(x)=(x+1, x^2+x+1, x^2, x^5+x^3+x^2+1)=x^{12}+x^8+x^7+x^6+x^5+1$. Поскольку $\deg \overline{A}_{PRNS}(x)>D$, многочлен содержит ошибку.

В соответствии с теоремой 1 могут быть обнаружены все одиночные ошибки, а также двойные ошибки по первому и второму, первому и третьему, второму и третьему модулям.

Тогда кандидатами будут

- $V_1(x)=x^7+x^5+x^3+x+1=(x+1, x^2+x, x^2, x^5+x^3+x^2+1)$ для которого $H_T=1$, $H_W=11$;
- $V_2(x)=x^6+x=(x+1, x^2+x+1, x^2, 1)$ для которого $H_T=1$, $H_W=8$;
- $V_3(x)=x^6+x^5+x^3+x^2+x=(x, x^2+x+1, x^2+x, x^5+x^3+x^2+1)$ для которого $H_T=2$, $H_W=9$.

В соответствии с методом наибольшего правдоподобия максимальный вес Хэмминга $H_W=11$ имеет кандидат $V_1(x)$, который соответствует числу без ошибки.

В общем случае добавление одного избыточного модуля позволяет только обнаружить одиночную ошибку, однако подход с использованием энтропии для полиномиальной системы классов вычетов позволил обнаружить и ряд двойных ошибок, а метод наибольшего правдоподобия позволяет исправить данную ошибку.

Использование многочленов в полях Галуа в полиномиальной системе классов вычетов может усложнить процесс написания вычислительных модулей. Другим подходом к использованию модулярного кода является система остаточных классов, для которой используются числовые значения.

Рассмотрим применение данных методов для системы остаточных классов.

3. Избыточная система остаточных классов для исправления ошибок

Еще одним эффективным представлением чисел при параллельной обработке является система остаточных классов (СОК). Если задан ряд положительных целых чисел $p_1, p_2, \dots, p_n$, называемых модулями или основаниями системы, то под системой остаточных классов понимается система, в которой целое положительное число представляется в виде набора остатков по выбранным основаниям $X=(x_1, x_2, \dots, x_n)$, где $x_i=|X|_{p_i}=X \bmod p_i$ для $i=1, 2, \dots, n$ [3]. Из теории чисел известно, что если модули p_i взаимно простые, то представление числа $X=\{x_1, x_2, \dots, x_n\}$ является единственным. При этом можно выполнять модульные операции сложения, вычитания и умножения с остатками независимо по каждому модулю [7].

Рассмотрим избыточную систему остаточных классов с одним избыточным модулем, т.е. n – общее число модулей, $r=1$ – количество избыточных модулей, $k=n-1$ – количество рабочих модулей. При этом $X<P=p_1 p_2 \dots p_{n-1}$, где P – динамический диапазон представления чисел. Добавление избыточного основания p_n в систему остаточных классов с модулями $\{p_1, p_2, \dots, p_{n-1}\}$ позволяет обнаружить ошибку, а именно, число корректно, если

лежит в диапазоне $[0, P)$, в случае нахождения числа в диапазоне $\left[P, \hat{P}\right)$, где $\hat{P} = P \cdot p_n$ – полный диапазон системы, число содержит ошибку.

Чтобы оценить, в какой диапазон входит число, необходимо найти его позиционную характеристику. Одним из методов получения позиционной характеристики является перевод из СОК в позиционную систему счисления с использованием метода на основе Китайской теоремы об остатках (КТО), по которой число X может быть получено из формулы

$$X = \left| \sum_{i=1}^{n} \hat{P}_i \cdot x_i \cdot \left| \hat{P}_i^{-1} \right|_{p_i} \right|_{\hat{P}}, \quad (1)$$

где $\hat{P}$ – полный динамический диапазон, $\hat{P}_i = \hat{P}/p_i$, $\left| \hat{P}_i^{-1} \right|_{p_i}$ – мультипликативная инверсия $\hat{P}_i$ по модулю p_i [8].

В общем случае добавление одного избыточного основания позволяет обнаружить одиночную ошибку. На основании теоремы 1 введем понятие энтропии для обнаружения ошибок большей кратности.

Энтропия модулей системы остаточных классов отражает количество информации, которое содержится в данном остатке, энтропия модуля равна $H(p_i) = \log_2 p_i$. Тогда энтропию модулей СОК можно записать в виде

$$h_E = \left(H(p_1), H(p_2), \dots, H(p_n)\right).$$

В [3] приведено утверждение, что если среди модулей СОК есть такие малые основания $p_{j,1}$, $p_{j,2}$, ..., $p_{j,t}$, для которых выполняется

$$\prod_{i=1}^{t} p_{j,i} < p_n,$$

то любые искажения в цифрах по нескольким или даже всем этим модулям превращают правильное число в неправильное и, следовательно, во всех случаях наличие искажений может быть обнаружено. Обобщим данное утверждение с помощью энтропии для системы с k рабочими модулями и $r = n - k$ избыточными модулями, где n общее количество модулей СОК. Введем теорему 2.

Теорема 2. Если задана система остаточных классов с n модулями $p_1, p_2, \dots, p_n$, где r – количество избыточных модулей, и $k = n - r$ – количество рабочих модулей, то для числа A, представленного в виде остатков $(a_1, a_2, \dots, a_n)$ и множества $\overline{I}$ остатков с ошибкой, ошибка может быть обнаружена, если выполняется условие

$$\sum_{i \in \overline{I}} H(p_i) \leq \sum_{j=1}^{r} H\left(p_{k+j}\right). \quad (2)$$

Доказательство:

Правильность числа в СОК с избыточным модулем означает, что число входит в рабочий диапазон, т.е. $A < \prod_{i=1}^{k} p_i = P$.

1) Пусть $\overline{I}$ – пустое множество и ошибок нет, тогда условие (2) примет вид $0 \leq \sum_{j=1}^{r} H\left(p_{k+j}\right)$, что выполняется для всех p_{k+j}, $j \in [1, r]$ и число A может быть восстановлено из КТО по формуле (1).

2) Рассмотрим случай с одним избыточным модулем и одиночной ошибкой, тогда условие (2) примет вид $H(p_i) \leq H(p_n)$, откуда из определения энтропии $\log_2 p_i \leq \log_2 p_n$, и $p_i < p_n$. Из определения правильности числа $A < P = \frac{\hat{P}}{p_n}$ и т.к. $p_i < p_n$, то $\frac{\hat{P}}{p_i} > \frac{\hat{P}}{p_n}$ и $A < \frac{\hat{P}}{p_n} < \frac{\hat{P}}{p_i}$. Поскольку число $\overline{A}$ содержит ошибку, то $\overline{a_i} \neq a_i$ и число $\overline{A}$ не может находиться в интервале

$\left[0, \frac{P}{p_i}\right)$, следовательно $\overline{A} > \frac{\hat{P}}{p_i}$ и тогда имеет место выражение $\overline{A} > \frac{\hat{P}}{p_n}$ и число $\overline{A}$ является неправильным.

3) Если возникли ошибки по нескольким основаниям $p_{i_1}, \dots, p_{i_l}$, то условие (2) примет вид $\sum_{\mathrm{j}=1}^{l} H\left(p_{i_j}\right) \le H(p_n)$, откуда $\log_2 p_{i_1} + \dots + \log_2 p_{i_l} \le \log_2 p_n$ и $\prod_{j=1}^{l} p_{i_j} \le p_n$. Рассмотрим произведение $\prod_{j=1}^{l} p_{i_j}$ как единое основание $\overline{p_i}$, получим $\overline{p_i} \le p_n$ и случай сводится к случаю 2, что означает, что любая ошибка по модулям $p_{i_j}, j \in [1, l]$ может быть обнаружена.

4) Если избыточных оснований несколько, $p_{k+1}, \dots, p_{k+r}$, то условие (2) примет вид $\sum_{\mathrm{j}=1}^{l} H\left(p_{i_j}\right) \le \sum_{j=1}^{r} H\left(p_{k+j}\right)$, откуда $\log_2 p_{i_1} + \dots + \log_2 p_{i_l} \le \log_2 p_{k+1} + \dots + \log_2 p_{k+r}$ и $\prod_{j=1}^{l} p_{i_j} \le \prod_{j=1}^{r} p_{k+j}$. Рассмотрим $\prod_{j=1}^{r} p_{k+j}$ как единое основание $\overline{p_n}$, то соблюдается условие $\overline{p_i} \le \overline{p_n}$ и случай сводится к случаю 2.

Таким образом, любая ошибка по модулям $p_{i_j}, j \in [1, l]$ может быть обнаружена.

Накладывая ограничения на избыточные модули СОК можно обнаружить ошибки большей кратности. Введем алгоритм 1 выбора позиций ошибок E, которые могут быть обнаружены. Для обнаружения ошибки нужно проверить комбинации ошибок от однократных до ошибок кратности $n-1$. Количество однократных ошибок равно C_n^1, количество двукратных ошибок C_n^2, и так далее, количество ошибок кратности $\mathrm{n}-1$ равно C_n^{n-1}, где C_n^k – количество сочетаний из n по k. Из бинома Ньютона $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$ можно получить, что количество ошибок кратности от 1 до $n-1$ равно $2^n - C_n^0 - C_n^n = \sum_{k=1}^{n-1} C_n^k = 2^n - 2$. $\langle h_E \cdot \mathrm{bin}(i) \rangle$ – скалярное произведение $h_E = \{H(p_1), H(p_2), \dots, H(p_n)\}$ и $\mathrm{bin}(i)$, где $\mathrm{bin}(i)$ – вектор из n нулей и единиц, полученный при переводе i в двоичную систему счисления.

Input: $\{p_1, p_2, \dots, p_n\}$,
$h_E = \{H(p_1), H(p_2), \dots, H(p_n)\}$
Output: E

1. $E = \{\}$
2. $T = \sum_{j=1}^{r} H\left(p_{k+j}\right)$
3. Для i от 1 до $2^n - 2$ выполнять:
   3.1. Если $\langle h_E \cdot \mathrm{bin}(i) \rangle \le T$, то
      3.1.1. Добавить $\mathrm{bin}(i)$ к E
4. Возвратить E

Алгоритм 1. Выбор позиций обнаруживаемых ошибок

Пример 2. Возьмем СОК с модулями $\{3, 5, 7, 37\}$ и одним избыточным модулем, для которых энтропии равны $h_E = (1.58, 2.32, 2.81, 5.21)$. Рассмотрим работу алгоритма 1. $T = 5.21$, тогда для $\mathrm{bin}(1) = \{0,0,0,1\}$ скалярное произведение $\langle h_E \cdot \mathrm{bin}(1) \rangle = H(p_n)$=5.21. Условие (2) выполняется, значит ошибка на позиции $\{0,0,0,1\}$ может быть обнаружена. Из алгоритма 1 выражение (2) выполняется для следующих сочетаний ошибок $\{p_1\}$, $\{p_2\}$, $\{p_3\}$, $\{p_4\}$, $\{p_1, p_2\}$, $\{p_1, p_3\}$, $\{p_2, p_3\}$, следовательно, ошибки на данных позициях могут быть обнаружены.

Рабочим диапазоном данной СОК является $P = 105$. Возьмем число $X = 10 = (1, 0, 3, 10)$ и введем ошибку по двум основаниям $E = (2, 0, 5, 0)$, получим число $\overline{X} = (0, 0, 1, 10)$. Используя формулу (1), получим $\overline{X} = (0,0,1,10) = 750$ и поскольку $750 > P = 105$, ошибка может быть обнаружена.

Важным приложением выражения (2) является возможность определения позиций обнаруживаемых ошибок, что позволит строить распределенные вычислительные системы с требуемыми корректирующими возможностями.

Очевидно, что количество избыточных модулей и их размеры обеспечивают необходимые возможности к обнаружению ошибок. Так, рассмотренный выше набор позволяет обнаружить ряд двойных ошибок, в то время как набор {3,5,7,8} обнаруживает только одиночные ошибки.

Рассмотрим применение веса Хэмминга и метода наибольшего правдоподобия из статьи [5] для системы остаточных классов. Для формирования кандидатов V_i во всех методах используется сравнение с рабочим диапазоном. Для нахождения кандидатов метода наибольшего правдоподобия выбираются все значения, входящие в рабочий диапазон, в которых изменены значения на позициях, найденных из выражения (2). В дальнейшем для каждого кандидата вычисляется вес Хэмминга и выбирается кандидат с наибольшим весом.

Пример 3. Для рассмотренного выше примера 2 с ошибочным числом $\overline{X} = (0,0,1,10)$ такими кандидатами будут числа $V_1 = (0,0,1,15)$, $V_2 = (1,0,3,10)$, $V_3 = (0,4,0,10)$, которые попадают в рабочий диапазон. Максимальное значение веса Хэмминга равно 7.53 для числа $V_2 = (1,0,3,10)$.

Однако если возникла ошибка $E = (2,0,4,0)$, то для полученного числа $\overline{X} = (0,0,0,10)$ кандидатами будут $V_1 = (0,4,0,10)$, $V_2 = (0,0,0,0)$, $V_3 = (1,0,3,10)$. Максимальное значение веса Хэмминга равно 9.60 для числа $V_1 = (0,4,0,10)$, что не соответствует исходному числу без ошибок.

Таким образом, метод наибольшего правдоподобия некорректно исправляет ошибки. Рассмотрим другой подход к исправлению ошибок, а также проанализируем исправляемые ошибки избыточной системой остаточных классов с одним избыточным основанием.

Другим подходом к локализации ошибки в системе остаточных классов является метод проекций. Проекцией X_i числа $X = (x_1, x_2, \dots, x_n)$ по модулю p_i будет число, полученное вычеркиванием цифры x_i в представлении X. Проекцией $X_{i,j}$ по основаниям p_i и p_j называется число, полученное из X вычеркиванием цифр по основаниям p_i и p_j. Если в упорядоченной системе остаточных классов с одним избыточным основанием проекция X_i числа X по модулю p_i удовлетворяет условию $X_i > \hat{P}/p_n$, то цифра x_i правильная, если возможна лишь одиночная ошибка [3].

При этом для правильного числа X все позиционные значения проекций равны между собой. Данное свойство может быть использовано в том случае, когда ряд проекций попадает в легитимный диапазон, и если среди них есть равные, то данное число и будет исходным, не содержащим ошибки.

Введение только одного избыточного основания в общем случае не позволяет локализовать ошибку.

Пример 4. Рассмотрим коррекцию ошибки методом проекций для СОК с одним избыточным основанием. Для СОК $\{3,5,7,37\}$ с числом $X = (1,0,3,10)$ введем ошибку $E = (0,1,0,0)$ и получим число $\overline{X} = (1,1,3,10)$. Поскольку $\overline{X} = 2341 > P = 105$, то число содержит ошибку. Построим проекции данного числа для позиций, найденных из выражения (2).

Тогда проекции, входящие в рабочий диапазон равны $\overline{X}_2 = (1,3,10) = 10$, $\overline{X}_4 = (1,1,3) = 31$, $\overline{X}_{1,2} = (3,10) = 10$, $\overline{X}_{2,3} = (1,10) = 10$. Поскольку часть проекций равна 10, то исходное число без ошибки равно $X = 10 = (1,0,3,10)$.

В [3] приведена теорема, согласно которой если избыточный модуль удовлетворяет условию $p_n > 2p_{n-1}p_{n-2}$, то ошибка по рабочему модулю может быть исправлена. Однако в данном случае система остаточных классов является несбалансированной, размерность избыточного основания более чем в 2 раза превышает размерность максимального рабочего модуля.

В статье [9] доказано уточнение, что исправление одиночной ошибки по рабочему модулю может быть осуществлено при $p_n > p_{n-1}p_{n-2}$.

4. Вычислительный эксперимент по обнаружению и исправлению ошибок

Рабочий диапазон $P = \prod_{i=1}^{k} p_i$ отражает разрешенные в данной системе числа, в то время как полный диапазон $\hat{P} = \prod_{i=1}^{n} p_i$ отражает все возможные числа в данной системе. При этом условием отсутствия ошибки числа A является выражение $A < P$, отсюда можно сделать вывод, что количество ошибочных значений равно $\hat{P} - P = P(\prod_{i=1}^{r} p_{k+i} - 1)$.

Количество одиночных ошибок по основанию p_i равно $p_i - 1$. Количество двойных ошибок по основаниям p_i и p_j равно $(p_i - 1)(p_j - 1)$. Количество ошибок больше кратности по основаниям p_{i_j} равно $\prod_j (p_{i_j} - 1)$. При этом ряд ошибок будет иметь сложную структуру, попадать в разрешенный диапазон и обнаружить их не будет возможности. В соответствии с выражением (2) можно определить позиции ошибок, которые гарантированно могут быть обнаружены, при этом могут быть обнаружены и дополнительные ошибки большей кратности, но существует вероятность ложного необнаружения ошибок.

Для исследование были взяты три набора модулей СОК с одним избыточным основанием: $\{3, 5, 7, 8\}$, в которой избыточное основание удовлетворяет выражению $p_n > p_{n-1}$; $\{3, 5, 7, 71\}$, в которой избыточное основание удовлетворяет выражению $p_n > 2p_{n-1}p_{n-2}$; $\{3, 5, 7, 37\}$, в котором избыточное основание удовлетворяет выражению $p_n > p_{n-1}p_{n-2}$. В ходе вычислительного эксперимента для всех чисел из рабочего диапазона были добавлены все допустимые ошибки, которые могут быть обнаружены в соответствии с выражением (2) и найдено количество исправляемых и неисправляемых ошибок.

Используя формулу (2) и вычисляя h_E для каждого набора модулей, получим, что

- набор $\{3, 5, 7, 8\}$ может обнаружить ошибки по следующим сочетаниям модулей $\{p_1\}, \{p_2\}, \{p_3\}, \{p_4\}$, всего 19 одиночных ошибок, при этом гарантированно ни одна ошибка не может быть исправлена;
- набор $\{3, 5, 7, 37\}$ может обнаружить ошибки по следующим сочетаниям модулей $\{p_1\}$, $\{p_2\}$, $\{p_3\}$, $\{p_4\}$, $\{p_1, p_2\}$, $\{p_1, p_3\}$, $\{p_2, p_3\}$, всего 92 ошибки, из них 48 одиночных и 44 двойных ошибки. Если учесть требование надежности избыточного основания, то система может обнаружить 56 ошибок по модулям $\{p_1\}$, $\{p_2\}$, $\{p_3\}$, $\{p_1, p_2\}$, $\{p_1, p_3\}$, $\{p_2, p_3\}$, 12 одиночных и 44 двойных. В этом случае и метод наибольшего правдоподобия и метод проекций гарантированно исправляют все одиночные ошибки;
- набор $\{3, 5, 7, 71\}$ может обнаружить ошибки по следующим сочетаниям модулей $\{p_1\}$, $\{p_2\}$, $\{p_3\}$, $\{p_4\}$, $\{p_1, p_2\}$, $\{p_1, p_3\}$, $\{p_2, p_3\}$, всего 126 ошибок, из них 82 одиночных и 44 двойных ошибок. Если учесть требование надежности избыточного основания, то система может обнаружить 56 ошибок по модулям $\{p_1\}$, $\{p_2\}$, $\{p_3\}$, $\{p_1, p_2\}$, $\{p_1, p_3\}$, $\{p_2, p_3\}$, 12 одиночных и 44 двойных. В этом случае и метод наибольшего правдоподобия и метод проекций гарантированно исправляют все одиночные ошибки.

Таким образом, все ошибки на позициях, удовлетворяющих выражению (2), могут быть обнаружены. Накладывание ограничений на избыточное основание позволяет исправить ошибки по рабочим модулям.

Рассмотрим результаты моделирования обнаружения и исправления ошибок.

Для набора модулей $\{3, 5, 7, 8\}$ на практике возможно обнаружение всех 19 одиночных ошибок, 110 из 128 двойных ошибок, 312 тройных ошибок из 356, 294 из 336 ошибок

кратности 4. Однако кроме случая гарантированного обнаружения одиночных ошибок, ошибки большей кратности могут иметь сложных характер и попадать в разрешенный диапазон, что приведет к ошибкам вычисления. Для случая исправления ошибок гарантированно исправить ошибку не представляется возможным, на практике метод наибольшего правдоподобия, как и метод проекций, в среднем позволяет исправить только 7 из 19 гарантированно обнаруживаемых одиночных ошибок. Если учесть требование надежности избыточного основания, то система может обнаружить ошибки по модулям $\{p_1\}$, $\{p_2\}$, $\{p_3\}$ и исправить 7 одиночных ошибок из 12 для обоих методов.

Для набора модулей $\{3, 5, 7, 37\}$ на практике возможно обнаружение всех 48 одиночных ошибок, 464 из 476 двойных ошибок, 1582 из 1632 тройных ошибок и 1682 из 1728 ошибок по всем 4 основаниям. При этом метод наибольшего правдоподобия позволяет исправить 13 из 48 одиночных и 24 из 44 двойных гарантированно обнаруживаемых ошибок. Если учесть требование надежности избыточного основания, то оба метода исправляют все одиночные ошибки и 24 из 44 двойных ошибок.

Для набора $\{3, 5, 7, 71\}$ на практике возможно обнаружение всех 82 одиночных ошибок, 872 из 884 двойных ошибок, 3083 из 3128 тройных ошибок и 3313 из 3360 ошибок по всем основаниям. При этом метод наибольшего правдоподобия позволяет исправить 34 из 82 одиночных и 37 из 44 двойных гарантированно обнаруживаемых ошибок. Если учесть требование надежности избыточного основания, то оба метода исправляют все одиночные ошибки и 24 из 44 двойных ошибок.

Как видно из результатов эксперимента, для исправления всех одиночных ошибок достаточно выполнения условия $p_n > p_{n-1}p_{n-2}$, что позволяет вдвое сократить размер надежного модуля, снизив тем самым разбалансировку модулей СОК и повысив производительность отказоустойчивой вычислительной системы.

5. Система надежного распределенного хранения в системе остаточных классов

Рассмотрим модель системы надежного распределенного хранения в системе остаточных классов, представленную четырьмя облаками, представленную на рис. 1. Пользовательская часть системы содержит блок преобразования позиционного числа X в систему остаточных классов с модулями $\{p_1, p_2, p_3, p_4\}$ и передачи данных в облака, а также блок приема данных, обнаружения и коррекции ошибки, и перевода из системы остаточных классов в позиционный код. При этом используемое количество облаков равно количеству модулей системы остаточных классов, и они хранят остатки x_i от деления исходного числа X на модули p_i, $x_i = |X|_{p_i}$. Данная система относится к взвешенным схемам разделения данных, при этом данные по модулям с большей энтропией размещаются в наиболее надежных облаках.

Рассмотрим систему, в которой могут возникать только одиночные и двойные ошибки, т.е. данные с одного или двух облаков могут быть потеряны или содержать ошибки. Будем рассматривать только гарантированно обнаруживаемые и исправляемые ошибки.

В этом случае для СОК с модулями $\{3, 5, 7, 8\}$ вероятность обнаружения и исправления однократных и двухкратных ошибок равны соответственно $P_{\text{обн}} = 0{,}129$ и $P_{\text{исп}} = 0$. Для СОК с модулями $\{3, 5, 7, 37\}$ вероятность обнаружения и исправления однократных и двухкратных ошибок равны соответственно $P_{\text{обн}} = 0{,}175$ и $P_{\text{исп}} = 0{,}023$. Для СОК с модулями $\{3, 5, 7, 71\}$ вероятность обнаружения и исправления однократных и двухкратных ошибок равны соответственно $P_{\text{обн}} = 0{,}130$ и $P_{\text{исп}} = 0{,}012$.

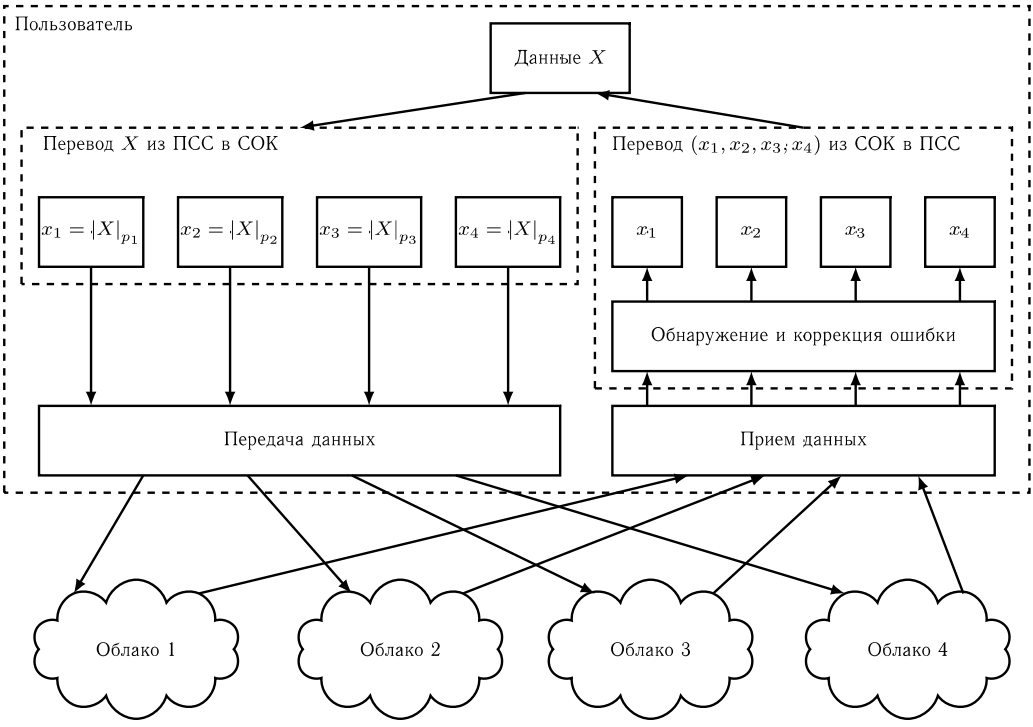

Рис. 1. Структура системы надежного распределенного хранения в системе остаточных классов

6. Заключение

В статье рассмотрена проблема обнаружения и исправления ошибок модулярного кода. Применение энтропийного подхода к обнаружению ошибок и метода наибольшего правдоподобия к локализации ошибок полиномиальной системы классов вычетов позволяет обнаружить и исправить ошибки большей кратности, по сравнению с классическими подходами. В то же время вычисления с многочленами требуют построения новой архитектуры вычислительных систем, что приводит к некоторым трудностям.

Использование энтропийного подхода к системе остаточных классов также позволяет повысить кратность обнаруживаемых ошибок и найти позиции ошибок, которые могут быть обнаружены данной системой. Доказана теорема, позволяющая определить позиции ошибок, которые точно могут быть обнаружены. Однако исправить все эти ошибки ни методом наибольшего правдоподобия, ни методом проекций не удается.

Если $p_n > p_{n-1}p_{n-2}$ и x_n – корректно, то код исправления ошибок позволяет исправить однократные ошибки и обнаружить двукратные ошибки. Вероятность обнаружения ошибки возрастает на 35% по сравнению с традиционными кодами исправления ошибок в модулярном коде.

Таким образом, эффективным для построения систем надежного распределенного хранения в системе остаточных классов является использование избыточной системы остаточных классов, в которой надежный избыточных модуль превышает произведение двух максимальных рабочих модулей. В этом случае система может обнаружить все однократные ошибки, а также ряд двухкратных ошибок по модулям, удовлетворяющим условию теоремы 2. Также система позволяет исправить все одиночные ошибки по рабочим модулям, что позволяет построить отказоустойчивую систему хранения данных.

Список литературы / References

[1]. Обнаружение и исправление ошибок в дискретных устройствах. Под ред. В.С. Толстякова. М.: Сов. радио, 1972. – 288 с. / Detection and correction of errors in discrete devices. Edited by V.S. Tolstyakov. Moscow: Sov. radio, 1972. - 288 p. (in Russian).

[2]. Стахов А.П. Введение в алгоритмическую теорию измерения. Москва: Сов. радио, 1977. – 288 с. / Stakhov, A.P. Introduction to the algorithmic theory of measurement / A.P. Stakhov. - Moscow: Sov. radio, 1977. - 288 p. (in Russian).

[3]. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М., Советское радио, 1968, 440 с. / Akushsky I. Ya., Yuditsky D. I. Computer arithmetic in residual classes. Moscow, Soviet Radio, 1968, 440 p. (in Russian).

[4]. Колмогоров А.Н. Три подхода к определению понятия «количество информации», Пробл. передачи информ., 1:1, 1965, с. 3–11 / Kolmogorov, A.N. Three approaches to the definition of the concept “quantity of information”. Probl. Peredachi Inf., 1965, 1, pp. 3–11. (in Russian).

[5]. Tchernykh A. et al. En-AR-PRNS: Entropy-Based Reliability for Configurable and Scalable Distributed Storage Systems //Mathematics. – 2021. – Т. 10. – №. 1. – С. 84.

[6]. Goh, V.T.; Siddiqi, M.U. Multiple error detection and correction based on redundant residue number systems. IEEE Trans.Commun. 2008, 56, 325–330. DOI: 10.1109/TCOMM.2008.050401

[7]. Chang C. H. et al. Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications //IEEE circuits and systems magazine. – 2015. – Т. 15. – №. 4. – С. 26-44. DOI: 10.1109/MCAS.2015.2484118

[8]. Aremu I. A., Gbolagade K. A. Redundant residue number system based multiple error detection and correction using Chinese remainder theorem (CRT) //Software Engineering. – 2017. – Т. 5. – №. 5. – С. 72-80. DOI: 10.11648/j.se.20170505.12

[9]. Gladkov A. et al. Modified Error Detection and Localization in the Residue Number System // Programming and Computer Software, 2022, Vol. 48, No. 8, pp. 598–605 DOI: 10.1134/S0361768822080126

Информация об авторах / Information about authors

Виктор Андреевич КУЧУКОВ – научный сотрудник отдела технологий программирования Института системного программирования РАН, младший научный сотрудник Северо-Кавказского центра математических исследований Северо-Кавказского федерального университета. Сфера научных интересов: высокопроизводительные вычисления, система остаточных классов, нейронные сети, цифровая обработка сигналов.

Viktor Andreevich KUCHUKOV is a researcher at the Department of Programming Technologies of the Ivannikov Institute for System Programming of the Russian Academy of Sciences, junior researcher at the North Caucasus Center for Mathematical Research of the North-Caucasus Federal University. Research interests: high-performance computing, residue number systems, neural networks, digital signal processing.