УДК 621.396
DOI 10.52575/2687-0932-2025-52-3-735-744
EDN YEHGIJ

Инновационные методы распараллеленной передачи и обработки измерительной информации, основанные на использовании конструктивной теории конечных полей

[1]Кукушкин С.С., [2]Кукушкин Л.С., [3]Махов Ф.С., [3]Головко М.В.
[1]АО «Военно-инженерная корпорация»,
Россия, 141092, Московской обл., г. Королёв, микрорайон Юбилейный, ул. Пионерская д.1-4,
[2]АО «Рязанское производственно-техническое предприятие»,
Россия, 390039, г. Рязань, ул. Интернациональная 12,
[3]Белгородский государственный национальный исследовательский университет,
Россия, 308015, г. Белгород, ул. Победы, 85,
adaptermetod@mail.ru, leofrontier@gmail.com, 1fmakhov@gmail.com, golovko_m@bsuedu.ru

Аннотация. Статья посвящена разработке новых методов передачи и обработки измерительной информации, что связано с необходимостью разрешения следующих противоречий. Объёмы передаваемой и получаемой измерительной информации быстро увеличиваются, что связано с растущими потребностями науки и техники. Но при этом значительно ухудшаются условия, в которых проводят измерения, погрешности измерительных приборов и систем не удовлетворяют предъявляемым требованиям, увеличивается интенсивность помехового фона. При этом возможности повышения основных показателей эффективности измерений за счёт аппаратных средств ограничены, а резервы используемых методов истощены. В этой ситуации основная надежда на повышение показателей точности и достоверности измерений оказывается связанной с обработкой полученной информации. Но, как это часто бывает, существующие методы и технологии обработки экспериментальных данных также оказываются не способными исправить полученные результаты. Поэтому появляется необходимость в разработке необычных (нетрадиционных) математических методов обработки данных измерений, чему и посвящена данная статья.

Ключевые слова: неопределённость данных измерений, искажения, вызванные действием помех, обработка данных, конструктивная теория конечных полей, система остаточных классов, регуляризация некорректных задач

Для цитирования: Кукушкин С.С., Кукушкин Л.С., Махов Ф.С., Головко М.В. 2025. Инновационные методы распараллеленной передачи и обработки измерительной информации, основанные на использовании конструктивной теории конечных полей. *Экономика. Информатика*, 52(3): 735–744. DOI 10.52575/2687-0932-2025-52-3-735-744. EDN YEHGIJ

Innovative Methods of Parallelized Transmission and Processing of Measurement Information Based on Using Constructive Finite Field Theory

[1]Sergej S. Kukushkin, [2]Leonid S. Kukushkin, [3]Fyodor S. Makhov, [3]Marina V. Golovko
[1]JSC Military Engineering Corporation,
1-4 Pionerskaya St., Yubileiny microdistrict, Korolyov, Moscow region 141092, Russia
[2]JSC Ryazan Production and Technical Enterprise, 12 Internatsionalnaya St., Ryazan 390039, Russia
[3]Belgorod State National Research University, 85 Pobedy St., Belgorod 308015, Russia
adaptermetod@mail.ru, leofrontier@gmail.com, 1fmakhov@gmail.com, golovko_m@bsuedu.ru

Abstract. The article is devoted to the development of new methods for transmitting and processing measurement information, which requires that the following contradictions should be resolved. The volumes

of transmitted and received measurement information are rapidly increasing, which is associated with the growing needs of science and technology. Meanwhile, the conditions in which measurements are carried out are considerably worsening, the errors of measuring devices and systems do not meet the requirements, and the intensity of interference background is increasing. At the same time, the possibilities of increasing the main indicators of measurement efficiency at the expense of hardware are limited, and the reserves of used methods are exhausted. In this situation, the main hope for increase of accuracy and reliability of measurements appears to be connected with processing of the received information. But, as it often happens, the existing methods and technologies of experimental data processing are also unable to correct the obtained results. Therefore, there is a need to develop unusual (non-traditional) mathematical methods of measurement data processing, which is the subject of this article.

Keywords: measurement data uncertainty, distortions caused by interference, data processing, constructive finite field theory, residual class system, regularization of incorrect problems

For citation: Kukushkin S.S., Kukushkin L.S., Makhov F.S., Golovko M.V. 2025. Innovative Methods of Parallelized Transmission and Processing of Measurement Information Based on Using Constructive Finite Field Theory. *Economics. Information technologies,* 52 (3): 735–744 (in Russian). DOI 10.52575/2687-0932-2025-52-3-735-744. EDN YEHGIJ

Введение

В современных условиях особую актуальность приобретает разработка новых методов измерений, передачи и обработки получаемых экспериментальных данных. Составляющие их основу противоречия ожесточаются, повышается уровень неопределённости измерений. Для их уменьшения разрабатываются новые методы и технологии повышения помехозащищённости как самих измерений, так и передачи их результатов в центр обработки и анализа.

Ранее использовавшиеся подходы исчерпали свои резервы, а синтезу необычных (нетрадиционных) технических решений мешают ограниченные возможности существующего математического аппарата. Предлагаются разработки, которые базируются на расширении области прикладного использования математических теорий высокого абстрактного уровня. К их числу относится классическая теория конечных полей и её приложения к области кодирования передаваемых данных и вычислений, составляющих основу их обработки [Кнут, 1977]. Основное её применение к области вычислений, известное под названием «система остаточных классов (СОК)», было ограничено отсутствием быстродействующих способов обратного преобразования данных, обладающих неопределённостью [Кукушкин, 2000]. Для того, чтобы их перевести при представлении образами-остатками в исходную область представления, использовался алгоритм китайской теоремы об остатках (КиТО). Но он обладал множеством недостатков, из-за чего методы обработки информации в системе остаточных классов (СОК) не нашли ожидаемого расширенного практического применения.

Объекты и методы исследования

В качестве объекта исследования выбран математический аппарат СОК. Наиболее известная область его применения связана с вычислениями [Торгашев, 1973]. Следующее направление прикладного его использования было связано с обеспечением помехоустойчивости передачи информации, обладающей внутренней избыточностью [Кукушкин, 2008]. Так, при передаче телеметрической информации (ТМИ) суть инновационных методов СОК заключалась в том, чтобы данные телеизмерений (ТИ) X_i, представленные (N = 2n = 10) - разрядным двоичным кодом, преобразовать в безызбыточный помехоустойчивый код C_i. Такая возможность, как показано на иллюстрации, приведенной на рис. 1, заключается в том, чтобы в результате сравнений по оптимально выбранным модулям $m_1 = 2^n - 1$ и $m_2 = 2^n + 1$ получить образы-остатки $b_{1i}(mod\ m_1)$ и $b_{2i}(mod\ m_2)$. При этом результат

безызбыточного помехоустойчивого кодирования $C_i = <b_{1i}(mod\ m_1), b_{2i}(mod\ m_2)>_2$ получают в результате их формального объединения в новое закодированное сообщение. Так, например, сообщение $X_i = <157>_2$, использующее для представления (N = 2n = 10) - разрядное кодовое слово при делении на оптимальные модули сравнения $m_1 = 2^5 - 1 = 31$ и $m_3 = 2^5 + 1 = 33$ даст остатки $b_1(mod\ m_1) = 2$ и $b_3(mod\ m_3) = 25$. Значение каждого из них может быть представлено 5-разрядным двоичным кодом (n = 5). После их формального объединения в новое кодовое слово, например, $C_i = <2;25>_2 = <00010,11001>_2$ получим при традиционном прочтении, учитывающем позиционную его структуру, следующий результат безызбыточного кодирования: $C_i = <00010,11001>_2 = <89>_{10}$. При этом, если следующее значение будет на «1» больше: $X_i = <90>_{10}$, то результат соответствующего дополнительного безызбыточного кодирования: $C_{i+1} = <00011,11010>_2 = <123>_{10}$ увеличится на значение минимального кодового расстояния $d_{min} = <1,00001>_2 = <33>_{10}$, представленного в метрике Евклида.

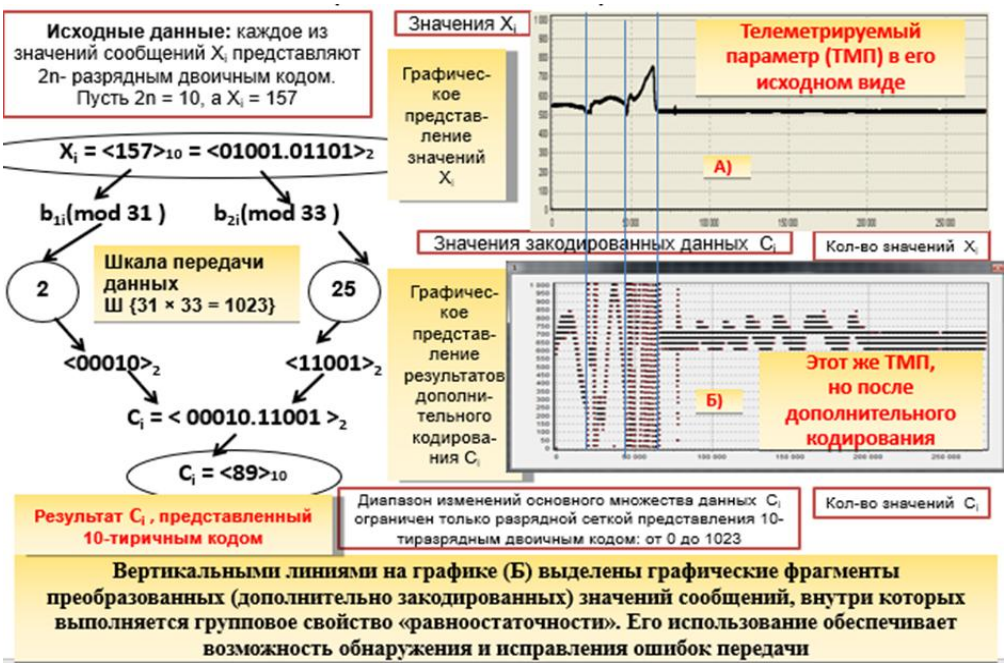

Рис. 1. Модель проблемно-ориентированного дополнительного безызбыточного помехоустойчивого кодирования передаваемой информации с использованием системы остаточных классов
Fig. 1. Model of problem-oriented additional non-redundant noise-resistant coding of transmitted information using the residual class system

При этом на приёмной стороне для восстановления предлагается использовать два декодера передаваемых сообщений, условно называемые «жёсткий» и «мягкий». Основу первого из них составлял алгоритм конструктивной теоремы об остатках (КтТО). Под его управлением работал «мягкий» декодер, предназначенный для обнаружения и исправления ошибок передачи ТМИ.

Проблемы, связанные с обработкой ТМИ, также потребовали совершенствования классической теории конечных полей Э. Галуа. Этому разделу разработки инновационных методов и технологий посвящены монографии [Кукушкин, 2008]. Их основная направленность заключалась в том, чтобы расширить возможности прикладного использования теории конечных полей. Одна из проблем заключалась в расширении областей числового представления данных [Roy, 1959]. Например, при кодировании информации значения сообщений должны быть представлены целыми числами: $\boldsymbol{x_i \in Z}$, в то время, как обработка данных ТМИ основывается на использовании рациональных чисел: $\boldsymbol{x_i \in Q}$. А в современных системах инфотелекоммуникации передача информации и её обработки представляют собой единое целое. Классическая теория конечных полей Э. Галуа также

предполагает, $x_i \in Z$. Поэтому и основное её применение было связано с помехоустойчивым кодированием информации. Это ограничение связано с известной процедурой обратного восстановления данных в их исходном представлении.

Известный алгоритм китайской теоремы об остатках (КиТО) требует подбора дополнительных значений в виде мультипликативно-обратных величин m_i', удовлетворяющих условию: $m_i \times m_i' \equiv 1(\text{mod } m_j)$. Рассмотрим случай использования двух модулей сравнения m_1 и m_2. В этом случае алгоритм китайской теоремы об остатках (КиТО) представляют в виде следующей формулы [Кнут, 1977]:

$$x_i = (m_1 \times m_1')b_{2i} + (m_2 \times m_2')b_{1i} \ (mod \ (m_1 \times m_2)), \quad (1)$$

где b_{1i} и b_{2i} – образы-остатки, полученные в результате сравнений по модулям m_1 и m_2, соответственно; m_1' и m_2' – мультипликативные элементы конечного поля, определяемые на основе следующих сравнений: $m_1 \times m_1' \equiv 1(\text{mod } m_2)$ и $m_2 \times m_2' \equiv 1(\text{mod } m_1)$.

Алгоритм КиТО сложен в вычислительном отношении. Об этом недостатке говорят, как об основной причине, ограничивающей возможности оперативного восстановления данных, представленных в СОК. Так, например, в [Романец, 1999] на с. 311 отмечено, что «китайская теорема об остатках является мощным криптографическим инструментом». Однако её прикладное применение ограничено, помимо сложности реализации, и другими недостатками [Wilkinson, 2005]. Она включает в себя сложные для определения и вычислений мультипликативные операции, предполагающие умножение значений образов-остатков на коэффициенты, представляющие собой большие числа. Так, при байтовом представлении исходных данных оптимальные модули сравнения равны: $m_1 = 15$, $m_2 = 17$, а мультипликативно-обратные элементы m_1' и m_2' находятся методом подбора подходящих значений. Для рассматриваемого случая $m_1' = m_2' = 8$. Тогда алгоритм (1) применительно к байтовым сообщениям будет иметь следующий вид:

$$X_i = 120b_{2i} + 136b_{1i} \ (mod \ 15 \times 17 = 255). \quad (2)$$

Но если для передачи использованы (N = 2n = 10) - разрядные двоичные слова, то выбранные оптимальные модули сравнения будут другими: $m_1 = 2^n - 1 = 31$, а $m_2 = 2^n + 1 = 33$. Тогда алгоритм КиТО будет записан, как:

$$X_i = 496b_{2i} + 528b_{1i} \ (mod \ 31 \times 33 = 1023). \quad (3)$$

Из представленных выражений (2) и (3) следует, что алгоритмы КиТО изменчивы. Входящие в них большие коэффициенты, на которые умножаются значения образов-остатков, постоянны только для определённого выбора модулей сравнения m_1 и m_2.

Этого основного недостатка лишён алгоритм конструктивной теоремы об остатках [Акушский, 1968]:

$$x = \begin{cases} \left.\begin{matrix} m_1\Delta/n + b_1, \Delta = b_1 - b_2 \geq 0 (m_1 < m_2); \\ m_1(m_2 + \Delta/n) + b_1, \Delta < 0 \end{matrix}\right\} n|\Delta \\ m_1(m_2 + \Delta/n) + b_1, \Delta < 0, \Delta > 0, n \dagger \Delta, n|(m_2 + \Delta); \\ m_1\left[m_2 - \frac{(m_2 - \Delta)}{n} + b_1\right], \Delta < 0, \Delta > 0, n \dagger \Delta, n|(m_2 - \Delta); \\ m_1(2m_2 + \Delta)/n + b_1, \Delta < 0, \Delta > 0, n \dagger \Delta, n|(2m_2 + \Delta); \\ m_1[m_2 - (2m_2 - \Delta)]/n + b_1, \Delta < 0, \Delta > 0, n \dagger \Delta, n|(2m_2 - \Delta); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (2k+1)m_1(km_2 + \Delta)/n + b_1, \Delta < 0, \Delta > 0, n \dagger \Delta, n|(km_2 + \Delta); \\ (2k+2)m_1[m_2 - (km_2 - \Delta)]/n + b_1, \Delta < 0, \Delta > 0, n \dagger \Delta \end{cases} \quad (4)$$

Обозначения $n\dagger\Delta$, $n/(km_2+\Delta)$, n/Δ, $n/(km_2-\Delta)$ ($k = 0, 1,..,$) читаются так: Δ не делится на n без остатка и $km_2 + \Delta$, $km_2 - \Delta$ делятся на n без остатка. Символ $\dagger$ означает, что $\Delta = b_1 - b_2$ не делится без остатка (или с остатком, не равным 0) на значение $n = |m_1 - m_2|$.

При модулях, отличающихся друг от друга на 1: ($n = |m_1 - m_2| = 1$), алгоритм восстановления с использованием КтТО наиболее прост:

$$x = \begin{Bmatrix} m_1\Delta/n + b_1, \Delta = b_1 - b_2 \geq 0 (m_1 < m_2) \\ m_1(m_2 + \Delta/n) + b_1, \Delta < 0 \end{Bmatrix} n|\Delta. \quad (5)$$

При модулях, отличающихся друг от друга на 2: ($n = |m_1 - m_2| = 2$), в алгоритм восстановления с использованием КтТО добавляется ещё одно звено вычислений:

$$x = \begin{Bmatrix} m_1\Delta/n + b_1, \Delta = b_1 - b_2 \geq 0 (m_1 < m_2); \\ m_1(m_2 + \Delta/n) + b_1, \Delta < 0; \\ m_1(m_2 + \Delta)/n + b_1, \Delta < 0, \Delta > 0, n \dagger \Delta, n/(m_2 + \Delta). \end{Bmatrix} n/\Delta \quad (6)$$

Если $n = |m_1 - m_2| = 3$, то адаптивная процедура восстановления будет дополнена еще одним (четвертым) звеном восстановления x. Благодаря этому свойству алгоритм восстановления x (2) становится адаптивным, что в итоге приводит к существенному уменьшению числа вычислительных операций и, как следствие этого, к повышению показателей оперативности и достоверности установления истинного значения величины x [Кукушкин, 2000].

Более того, алгоритм (2) может быть использован и в случае, когда обрабатываемые и восстанавливаемые данные представлены в области рациональных чисел: $\boldsymbol{b_i \in Q}$ и $\boldsymbol{x_i \in Q}$. Такая возможность связана с тем, что многозвенные формулы восстановления значений $\boldsymbol{x_i \in Q}$ используют в качестве основы структуру одной из основных теорем арифметики:

$$x_i = m_j l_i + b_i, \quad (7)$$

где x_i – делимое, m_j – делитель, l_i – частное, а b_i – остаток.

Несмотря на то, что она сформулирована для случая целых чисел ($\boldsymbol{x_i}$, $\boldsymbol{m_j}$, $\boldsymbol{l_i}$, $\boldsymbol{b_i \in Z}$), она оказывается справедливой и для случая, когда $\boldsymbol{x_i \in Q}$ и $\boldsymbol{b_i \in Q}$. Но это возможно тогда, когда для восстановления используют адаптивный алгоритм восстановления, основу которого составляет конструктивная теорема об остатках (КтТО).

В этом случае исходные данные $n = |m_1 - m_2|$ и $\Delta = b_1 - b_2$ также целые числа ($\boldsymbol{n, \Delta \in Z}$), при $\boldsymbol{x_i \in Q}$ и $\boldsymbol{b_i \in Q}$.

Покажем это на численном примере, составляющем основу решения следующего сравнения:

$$\begin{aligned} x &= m_1 l_1 + b_1 \\ x &= m_2 l_2 + b_2. \end{aligned} \quad (8)$$

Предположим, что $x = 539{,}21$, а модули сравнения $m_1 = 31$, $m_2 = 33$. Тогда $b_1 = 12{,}21$, а $b_2 = 11{,}21$. Определяем исходные данные для восстановления на основе КтТО: $n = |m_1 - m_2| = |31 - 33| = 2$ и $\Delta = b_1 - b_2 = 12{,}21 - 11{,}21 = 1$. Они свидетельствуют о том, что в формуле (4) для восстановления значения $x_i = 539{,}21$ на основе известных образов-остатков необходимо воспользоваться третьим звеном, так как результат деления $\Delta = 1$ на $n = 2$ не относится к целым числам ($\mathbf{Z}$):

$$x = m_1 \frac{(m_2 + \Delta)}{n} + b_1. \quad (9)$$

Подставляя данные, получим: $x = 31 \times 17 + 12{,}21 = 539{,}21$. Проверяем достоверность полученного результата на основе замены индексов в формуле (9) 1 на 2: $x = 33 \times 16 + 11{,}21 = 539{,}21$. Результаты вычислений совпали, следовательно, ошибки при вычислениях не было.

Проверим, что будет при использовании алгоритма китайской теоремы об остатках. Вначале посмотрим, что даст решение системы сравнений при приёме (N=2n)-разрядных двоичных сообщений X_i, дополнительно закодированных на передающей стороне с использованием образов-остатков

$$C_i^{(1)} = <b_{1i}(mod\ m_1),\ b_{2i}(mod\ m_2)>2,$$
$$X_i = 496b_{2i} + 528b_{1i}\ (mod\ 31 \times 33 = 1023), \qquad (10)$$

при представлении исходных значений целыми числами: $X_i = 539$; $b_{1i} = 12$, и $b_{2i} = 11$ (пример и иллюстрации такого дополнительного кодирования в системе остаточных классов (СОК) приведены на рис. 1).

Выполним вычисления: 1) $X_i = 496b_{2i} + 528b_{1i} = 496\times11 + 528\times12 = 5456 + 6336 = 11792$; 2) найдем остаток b от деления числа 11792 на укрупнённый модуль сравнения $31 \times 33 = 1023$ – он равен значению $x = b = 539$. Сравнивая с исходным значением сообщения, которое было дополнительно закодировано в системе остаточных классов (СОК) и передано в канал связи, убеждаемся, что результат восстановления является верным. При этом необходимо отметить, что влияние помех, которые могут привести к искажению результата восстановления, не учитывалось.

Также все исходные данные были представлены целыми числами. Это условие выполняется при кодировании передаваемой информации. Но для последующей обработки полученных данных, ориентированной, например, на их фильтрацию (сглаживание), существующий математический аппарат классической теории Э. Галуа нуждается в доработке. Такая потребность появляется в связи с тем, что исходные данные, подвергаемые обработке, принадлежат области рациональных чисел $\boldsymbol{Q}$. Например, если данные телеизмерений X_i, графики изменения которых во времени были представлены целыми числами, принадлежащими $\mathbf{Z}$ (рис. 1), то при приёме, используя тарировочные характеристики датчиков, их преобразуют, в общем случае, в числа рациональные $\boldsymbol{Q}$.

Но для того чтобы убедиться, будет ли при этом возможность использования математического аппарата образов-остатков, посмотрим, что при этом даст результат восстановления на основе алгоритма китайской теоремы об остатках (КиТО). Воспользуемся при этом ранее заданными исходными данными: $x = 539{,}21$, модулями сравнения $m_1 = 31$, $m_2 = 33$, а также образами-остатками: $b_1 = 12{,}21$ и $b_2 = 11{,}21$.

Повторим вычисления при задании новых условий: 1) $X_i = 496b_{2i} + 528b_{1i} = 496\times11{,}21 + 528\times12.21 = 5560{,}16 + 6446{,}72 = 12006{,}88$; 2) найдем остаток b от деления числа 12006,88 на укрупнённый модуль сравнения $31 \times 33 = 1023$. В результате получим остаток $b = 753{,}88$. Сравнивая с исходным значением $x = 539{,}21$, видим значительное его отличие от того, что было получено на основе алгоритма КиТО. Отсюда следует вывод, который и до вычислений был очевидным: существующая теория конечных полей не может быть использована при разработке инновационных технологий обработки информации: она ориентирована на область представления данных в целых числах ($\mathbf{Z}$). В этом заключается её существенное ограничение. Но оно исчезает, как только алгоритм КиТО заменяем на алгоритмы КтТО [Кукушкин, 2000]. Тогда, оказывается, появляется и новый «мощный криптографический инструмент», о котором мечтали выдающиеся учёные, занимающиеся проблемами защиты информации [Романец, 1999]. Он существенно проще, является адаптивным, поскольку количество звеньев формулы (2) определяется абсолютной разностью между модулями сравнения $n = |m_1 - m_2|$. При передаче информации их выбирают, исходя из разрядности (N = 2n) двоичного кода, которым представлены передаваемые данные и сообщения X_i. Они являются оптимальными при $m_1 = 2^n - 1$, $m_2 = 2^n + 1$. В этом случае $n = |m_1 - m_2| = 2$. Тогда в соответствии с известным алгебраическим тождеством: $m_1 \times m_2 = (2^n - 1)(2^n + 1) = 2^{2n} - 1 = 2^N - 1$. А это означает, что произведение выбранных модулей сравнения обеспечивает возможность однозначного восстановления всех значений N - разрядного двоичного кода. При выбранных модулях

сравнения $m_1 = 2^5 - 1 = 31$ и $m_2 = 2^5 + 1 = 33$ диапазон восстанавливаемых значений сообщений определяется шкалой однозначного их представления (Ш): Ш = 0 … 1023, что совпадает с аналогичным показателем для десятиразрядного двоичного кода N: N = 2n = 10.

Также необходимо отметить и ещё одну особенность восстановления дополнительно закодированных данных при передаче информации. Она связана с эффектом дублирования передаваемых данных при их дополнительном кодировании образами-остатками [Сухорученко, 1995]. Для подтверждения этой особенности воспользуемся примером графического представления исходного телеметрического параметра (ТМП), представленного дискретными его отчётами, полученными в результате применения теоремы В.А. Котельникова о дискретизации [Кукушкин, 2008]. В этом случае каждое из передаваемых 10 - разрядных сообщений X_i подвергают, как это было показано на рис. 1, дополнительному кодированию. Вначале находят значения образов-остатков $b_{1i}(mod\ m_1)$ и $b_{2i}(mod\ m_2)$, которые объединяют в такое же по разрядности двоичное слово: $C_i^{(1)} = <b_{1i}(mod\ m_1), b_{2i}(mod\ m_2)>_2$.

При приёме образы-остатки $b_{1i}(mod\ m_1)$ и $b_{2i}(mod\ m_2)$ выделяют на основе разделения принятых закодированных сообщений $C_i^{(1)}$ на старшее $A_i = b_{1i}(mod\ m_1)$ и младшее $B_i = b_{2i}(mod\ m_2)$ полуслова. Эта операция составляет основу «жёсткого» декодирования данных на основе алгоритмов КтТО, что и было рассмотрено ранее. Под его управлением работает «мягкий» декодер значений дополнительно закодированных данных и сообщений. Но разделение на старшее $A_i = b_{1i}(mod\ m_1)$ и младшее $B_i = b_{2i}(mod\ m_2)$ полуслова также необходимо для получения второго инвариантного результата кодирования данных в СОК $C_i^{(2)} = <b_{2i}(mod\ m_2), b_{1i}(mod\ m_1)>_2$. Его использование при передаче могло оказаться неприемлемым из-за ограничений на пропускную способность канала связи. Но после приёма сообщений $C_i^{(1)}$ нет таких препятствий, поэтому в результате перестановки полуслов $A_i = b_{1i}(mod\ m_1)$ и $B_i = b_{2i}(mod\ m_2)$ может быть сформировано и дополнительное закодированное сообщение $C_i^{(2)} = <b_{2i}(mod\ m_2), b_{1i}(mod\ m_1)>_2$, что и показано на примере графических представлений на рис. 2. В результате такой операции исходный телеметрируемый параметр (ТМП) X_i^*, который при традиционной передаче был бы искажён помехой и восстановлен при приёме с ошибками ε_i^*: $X_i^* = X_i + \varepsilon_i^*$, может быть представлен в виде двух версий представления данных в СОК: $C_i^{(1)} = <b_{1i}(mod\ m_1), b_{2i}(mod\ m_2)>_2$ и $C_i^{(2)} = <b_{2i}(mod\ m_2), b_{1i}(mod\ m_1)>_2$ (рис. 2). При этом одна из них, например, $C_i^{(1)}$ была передана по каналу связи, а вторая – $C_i^{(2)}$ – синтезирована на приёмной стороне.

Затем каждая из закодированных копий в СОК была подвергнута обработке с использованием алгоритма сглаживания (фильтрации) данных, основу которого, например, составляет метод наименьших квадратов К. Гаусса. Результаты помехоустойчивого кодирования $C_i^{(1)*}$ и $C_i^{(2)*}$, искажённые в результате действия помех, имеют различные значения минимального кодового расстояния в метрике Евклида d_{min}.

Из графических представлений изменения во времени значений $C_i^{(1)*}$ и $C_i^{(2)*}$ следует, что они, копируя друг друга, отличаются тем, что их значения не совпадают (не являются простым повторением, как это имеет место при традиционном дублировании данных). Также не совпадают по времени и их разрывы значений дополнительно закодированных значений ТМП первого рода, определяемые на основе неравенств:

$$\begin{aligned} \Delta C_i^{(1)*} &= |\, C_i^{(1)*} - C_{i+1}^{(1)*}| \geq 0{,}8 \times 2^N \\ \Delta C_i^{(2)*} &= |\, C_i^{(2)*} - C_{i+1}^{(2)*}| \geq 0{,}8 \times 2^N, \end{aligned} \qquad (11)$$

где N – число разрядов двоичных слов, используемых для передачи сообщений.

Использование существующих информационных технологий фильтрации данных также упрощается за счёт того, что на основе неравенств (11) определяют моменты разрывов дополнительно закодированных значений $C_i^{(1)*}$ и $C_i^{(2)*}$. Таким образом определяют интервалы сглаживания (фильтрации): они должны находиться между соседними разрывами, определяемыми с использованием неравенств (11).

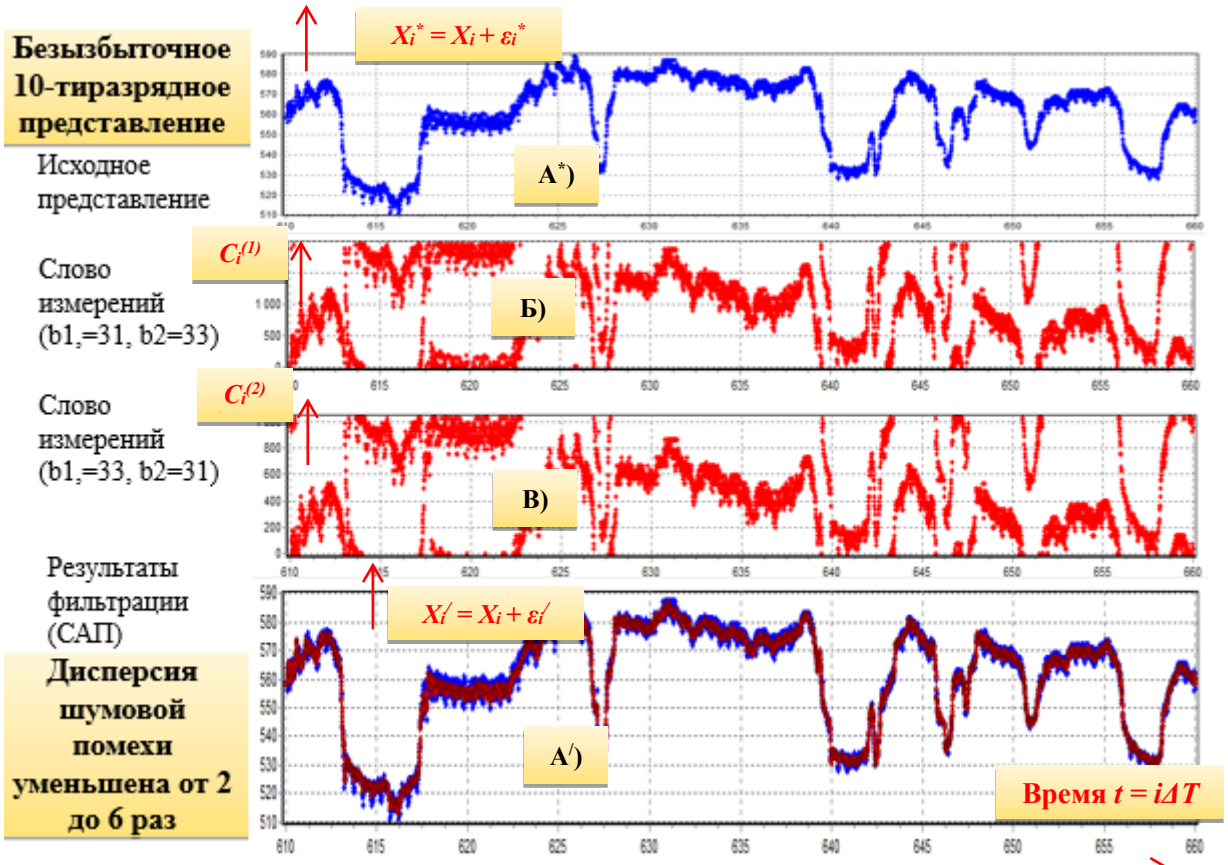

Рис. 2. Результаты графического изменения во времени значений телеметрируемого параметра одного и того же ТМП: при традиционной передаче $X_i^* = X_i + \varepsilon_i^*$(A*), а также при дополнительном кодировании в СОК в двух вариантах: переданном $C_i^{(1)*} = <b_{1i}(mod\ m_1), b_{2i}(mod\ m_2)>_2$ (Б) и дополнительно сформированном при приёме $C_i^{(2)*} = <b_{2i}(mod\ m_2), b_{1i}(mod\ m_1)>_2$ (В) с результатами совместной их обработки с использованием метода наименьших квадратов

Fig. 2. Results of graphical time variation of the telemetered parameter values of the same TMP: in case of traditional transmission $X_i^* = X_i + \varepsilon_i^*$(A*), as well as with additional encoding in the SOC in two versions: transmitted $C_i^{(1)*} = <b_{1i}(mod\ m_1), b_{2i}(mod\ m_2)>_2$ (Б) and additionally generated at the reception $C_i^{(2)*} = <b_{2i}(mod\ m_2), b_{1i}(mod\ m_1)>_2$ (В) with the results of their joint processing using the least squares method

Результаты кодирования $C_i^{(1)*}$ и $C_i^{(2)*}$ также могут отличаться тем, что при обработке отсутствует как таковая необходимость в экономии количества разрядов двоичного кода, который используют при представлении их значений данных при передаче. Необходимость в этом появляется только при передаче, когда особо актуальной становится проблема сжатия данных с целью уменьшения требований к пропускной способности каналов связи [Фалеев, 2015].

Как показали проведенные экспериментальные исследования с использованием реальной теплеметрической информации (ТМИ) в результате искусственного увеличения на приёмной стороне копий данных, закодированных в СОК, дисперсия шума, искажающего восстановленный ТМП, уменьшается от 2 до 6 раз (рис. 2). График A/ отфильтрованного ТМП представлен на фоне традиционно получаемого красным цветом.

Заключение

В настоящее время существенное научное и практическое значение для совершенствования информационных процессов передачи и обработки информации приобретает конструктивная теория конечных полей. Она, как показывают частные исследования, приведенные в статье, способствует расширению возможности прикладного применения классической теории Э. Галуа. В статье показано, как может быть полезно использована СОК по новому назначению: для передачи ТМИ и её обработки. Отмечается, что

эта технология может быть единой и взаимодополняющей. С одной стороны, передача ТМИ на основе дополнительного кодирования с использованием образов-остатков не только позволяет обнаруживать и исправлять ошибки телеизмерений (ТИ). Она обеспечивает повышение оперативности обработки и уменьшения дисперсии шума, искажающего значения ТМП при использовании алгоритмов фильтрации. Новизна предлагаемого подхода заключается также и в том, что обработке, в том числе и с целью сглаживания (фильтрации) данных, могут подвергаться сами значения образов-остатков. Полученные при этом по каждому из модулей сравнения класс-решения задачи фильтрации объединяют на основе алгоритмов КтТО. В результате этого, как показали результаты экспериментальных исследований, дисперсия шумовой составляющей может быть существенно уменьшена. Также при этом имеются и другие возможности повышения эффективности передачи информации и её обработки. Они связаны с обнаружением и исправлением ошибок передачи.

Список литературы

Акушский И.Я., Юдицкий Д.И. 1968. Машинная арифметика в остаточных классах. М.: Сов. Радио, 140.

Кнут Д. 1977. Искусство программирования для ЭВМ. Т. 2 Получисленные алгоритмы. М.: Мир, 724.

Кукушкин С.С. 2000. Конечные поля и информатика. в 2-х томах, т. 1. Методы и алгоритмы, классические и нетрадиционные, основанные на использовании конструктивной теоремы об остатках. М.: МО РФ, 260.

Кукушкин С.С., Гладков И.А., Чаплинский В.С. 2008. Методы и информационные технологии контроля состояния динамических систем. М.: МО РФ, 328.

Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. 1999. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 328.

Торгашев В.А. 1973. Система остаточных классов и надёжность ЦВМ. М.: Сов. Радио, 120.

Сухорученко Б.И., Меньшиков В.А. 1995. Методы анализа характеристик летательных аппаратов. М.: Машиностроение, 368.

Фалеев О.В. 2015. Принципы реализации параллельной обработки измерительной информации. *Вестник РГРТУ*, № 54. Часть 2: 23–37.

Roy B. 1959. Transitivité et connexité. C. R. Acad. Sci. Paris. 249: 216–218.

Wilkinson B., Allen M. 2005. Parallel programming techniques and applications using networked workstations and parallel computers. Pearson Education, 468.

References

Akushsky I.Ya., Yuditsky D.I. 1968. Machine Arithmetic in Remainder Classes. Moscow: Sov. Radio, 140.

Knuth D. 1977. The Art of Computer Programming. Vol. 2. Seminumerical Algorithms. Moscow: Mir, 724.

Kukushkin S.S. 2000. Finite Fields and Computer Science. in 2 volumes, vol.1. Methods and algorithms, classical and non-traditional, based on the use of the constructive remainder theorem. M.: MO RF, 260.

Kukushkin S.S., Gladkov I.A., Chaplinsky V.S. 2008. Methods and information technologies of monitoring the state of dynamic systems. M.: MO RF, 328.

Romanets Yu.V., Timofeev P.A., Shangin V.F. 1999. Information protection in computer systems and networks. M.: Radio and communication, 328.

Torgashev V.A. 1973. The System of Remainder Classes and the Reliability of the Computer. Moscow: Sov. Radio, 120.

Sukhoruchenko B.I., Menshikov V.A. 1995. Methods of Aircraft Characteristics Analysis. Moscow: Mashinostroenie, 368.

Faleev O.V. 2015. Principles of implementing parallel processing of measurement information. *Vestnik RGRTU*, No. 54. Part 2: 23–37.

Roy B. 1959. Transitivité et connexité. C. R. Acad. Sci. Paris. 249: 216–218.

Wilkinson B., Allen M. 2005. Parallel programming techniques and applications using networked workstations and parallel computers. Pearson Education, 468.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 01.08.2025
Поступила после рецензирования 04.09.2025
Принята к публикации 05.09.2025

Received August 01, 2025
Revised September 04, 2025
Accepted September 05, 2025

ИНФОРМАЦИЯ ОБ АВТОРАХ

Кукушкин Сергей Сергеевич, доктор технических наук, профессор, заслуженный изобретатель Российской Федерации, ведущий научный сотрудник АО «Военно-инженерная корпорация», г. Королёв, Московская обл., Россия

Кукушкин Леонид Сергеевич, научный сотрудник АО «Рязанское производственно-техническое предприятие», г. Рязань, Россия

Махов Федор Сергеевич, магистрант кафедры информационно-телекоммуникационных систем и технологий, Белгородский государственный национальный исследовательский университет, г. Белгород, Россия

Головко Марина Викторовна, ассистент кафедры информационно-телекоммуникационных систем и технологий, Белгородский государственный национальный исследовательский университет, г. Белгород, Россия

INFORMATION ABOUT THE AUTHORS

Sergey S. Kukushkin, Doctor of Technical Sciences, Professor, Honored Inventor of the Russian Federation, Leading Researcher at the JSC Military Engineering Corporation, Korolev, Moscow region, Russia

Leonid S. Kukushkin, Researcher at JSC Ryazan Production and Technical Enterprise, Ryazan, Russia

Makhov F. Sergeevich, Master's Student of the Department of Information and Telecommunication Systems and Technologies, Belgorod State National Research University, Belgorod, Russia

Marina V. Golovko, Assistant at the Department of Information and Telecommunication Systems and Technologies, Belgorod State National Research University, Belgorod, Russia