УДК 629.7.05, 621.398

© Кукушкин С.С., Кузнецов В.,И.
Kukushkin S., Kuznetsov V.

К ОБОСНОВАНИЮ ВИДА ЗАКОНА РАСПРЕДЕЛЕНИЯ НОРМАЛЬНО РАСПРЕДЕЛЁННЫХ СТАТИСТИЧЕСКИХ ДАННЫХ ПРИ ИХ ПРЕДСТАВЛЕНИИ ОБРАЗАМИ-ОСТАТКАМИ

TO THE SUBSTANTIATION FORM OF THE DISTRIBUTION OF NORMAL DISTRIBUTIONS STATISTICS AT THEIR PORTRAYALS RESIDUES

Аннотация. *В статье рассмотрены теоретические аспекты, относящиеся к реализации новой формы представления общего алгоритма конструктивной теоремы об остатках для восстановления данных, представленных образами-остатками, а также преобразования нормального закона распределения статистических данных при их представлении образами–остатками. Изложенный материал базируется на результатах исследований, полученных при выполнении ОКР «Универсал-ТМИ», головным исполнителем которого является ОАО «ВИКор».*

Annotation. *The article deals with theoretical aspects related to the implementation of the new format for the general algorithm constructive remainder theorem to recover data submitted images-residues, as well as the transformation of a normal distribution of statistics in their portrayals-residues. The material is based on research results obtained during implementation of the ROC "Universal TMI", which is the main executor of "Vicor".*

Ключевые слова. *Измерение, модуль сравнения, нормальное распределение, образ-остаток, помехоустойчивое кодирование, статистические данные, теорема об остатках, характеристическая функция.*

Key words. *Measurement, comparison module, normal distribution, image-residue noiseless coding, statistics, remainder theorem, the characteristic function.*

1. Общетеоретические положения

Актуальность. Современная информатика ориентирована на развитие тех областей знаний, которые становятся все более важными для современного общества. Возможности ее дальнейшего развития связаны с поиском новых резервов для повышения эффективности комплексов радиотехнических измерений и систем передачи информации. Прежние резервы уже практически исчерпаны, а поиск новых нуждается в усилении творческих возможностей человека. Такую уникальную возможность предоставляет прикладная математика, которая способна адаптировать и развить в выбранном прикладном направлении такие современные абстрактные теории, как теория чисел и теория конечных полей Э. Галуа. Эта область развития становится все более актуальной для различных технических приложений.

Основные понятия и ретроспективный анализ значимости научного направления в сравнении с другими традиционно используемыми подходами.

Истоки представляемого научного направления имеют непосредственное отношение к древнему Китаю. Эмпирически было обнаружено свойство остатков mod, получающихся в результате деления одного числа x_j (делимого) на другое m_i (делитель), называемое в теории конечных полей Галуа модулем сравнения. Было показано, что над остатками можно выполнять те же действия

Кукушкин Сергей Сергеевич – доктор технических наук, профессор, ведущий научный сотрудник, ФБУ «4 ЦНИИ» Минобороны России;
Кузнецов Валерий Иванович – доктор технических наук, старший научный сотрудник, ведущий научный сотрудник, ОАО «Военно-инженерная корпорация», тел. 8 (495) 399-98-19.

Kukushkin Sergey – doctor of technical sciences, professor; leading researcher, FBU «4 CRI» Russian Defense Ministry;
Kuznetsov Valery –doctor of technical sciences, senior researcher, JSC "Military engineering corporation", tel. 8 (495) 399-98-19.

A сложения, вычитания и умножения, что и над исходными целочисленными значениями $A(x_j)$, а полученный при этом результат $A(b_{ij})$ совпадает с данными сравнения $A(x_j) \equiv b_{ij} (\mathrm{mod}\, m_i)$. В современной математической терминологии это *свойство гомоморфизма.* Поэтому и остатки b_{ij}, называют *гомоморфными образами числа X* [1–5].

Проблема заключалась в том, как на основе остатков b_{ij} восстановить значение $A(x_j)$, не выполняя традиционные вычисления с числами x_j.

Впервые она была решена великим математиком Л .Эйлером. Первый алгоритм восстановления стал возможным благодаря изобретению им функции $\varphi(m_j)$ [2]:

$$\mathbf{X} = \sum_{s=1}^{k} b_i M_i^{\varphi(m_i)} (\mathrm{mod}\, \Pi m_i), \qquad (1)$$

где $\varphi(m_j)$ – функция Эйлера.

В честь особых заслуг математиков древнего Китая в области теории чисел алгоритм (1) был назван Эйлером *китайской теоремой об остатках.*

Второе формализованное представление алгоритма обратного восстановления было получено после появления теории конечных полей Галуа на основе одного из основных его понятий – мульпликативно-обратного элемента $M_s^{/}$ [2– 5]

$$\mathbf{X} = \sum_{s=1}^{k} M_s M_s^{/} (\mathrm{mod} \prod_{i=1}^{k} m_i);$$
$$\prod_{i=1}^{k} m_i = M_s m_s; \quad M_s M_s^{/} \equiv 1 \left(\mathrm{mod}\, m_i\right). \qquad (2)$$

Однако и первой и второй форме представлений *китайской теоремы об остатках* присущи недостатки, связанные с большим объемом вычислений. Следствием этого являются низкие показатели оперативности восстановления. Достаточно часто получается, что при практическом использовании тот выигрыш, который достигается за счет уменьшения разрядности образов-остатков, съедается большими вычислительными затратами на восстановление.

Этот недостаток частично был устранен в рекуррентном алгоритме (3), который был получен Х.Л. Гарнером в 1958 г. и носит его имя [3].

Теорема Гарнера приводит к следующему алгоритму восстановления:

$$\mathbf{X} = \vartheta_k m_{k-1} m_{k-2} \ldots m_1 + \ldots + \vartheta_3 m_2 m_1 + \vartheta_2 m_1 + \vartheta_1, \qquad (3)$$

где $\vartheta_1 = b_1$; ;

$$\vartheta_2 = (b_2 - \vartheta_1) C_{12} \left(\mathrm{mod}\, m_2\right);$$
$$\vartheta_3 = \left((b_2 - \vartheta_1) C_{13} - \vartheta_2\right) C_{23} \left(\mathrm{mod}\, m_3\right)$$

$$\ddot{\vartheta}_k = \left(\left(\ldots (b_k - \vartheta_1) C_{1k} - \vartheta_2\right) C_{2k} - \ldots - \vartheta_{k-1}\right) C_{(k-1)k} \left(\mathrm{mod}\, m_k\right);$$

$C_{ij} m_i \equiv 1 \left(\mathrm{mod}\, m_j\right)$, C_{ij} – мульпликативно-обратный элемент.

Основные недостатки известных теорем об остатках заключены в следующем:

• возможности их использования только при взаимно простых модулях сравнения $(m_i, m_j)=1$;

• в необходимости нормализации результата вычислений, заключающегося в нахождении его остатка по модулям $m_i, i = 1,2,\ldots,k$ или произведению модулей $\prod_{i=1}^{k} m_i$;

• в сложности алгоритмов восстановления и значительном времени вычислений.

Кроме того, необходимы подготовительные вычисления для получения новых исходных данных при смене модулей сравнения m_i. В этом случае мульпликативно-обратные элементы необходимо рассчитывать заново. При этом они не могут быть найдены при составных модулях сравнений, когда $(m_i, m_j) \neq 1$ [2–5].

2. Новая форма представления общего алгоритма конструктивной теоремы об остатках для восстановления данных, представленных образами-остатками

Проведенные исследования показали [12–19], что использование мультипликативно-обратного элементов M_{ij} в алгоритме китайской теоремы об остатках второй формы представления и C_{ij} в алгоритме теоремы Х.Л. Гарнера, обеспечивая компактность аналитической записи, приводит ко многим недостаткам, которые ограничивают возможности расширенного использования при решении прикладных задач. В ряде случаев, относящихся к радиотехническим измерениям и передаче информации в высокоскоростных каналах связи это ограничение приводит к невозможности применения известных алгоритмов китайской теоремы об остатках и теоремы Х.Л. Гарнера.

В 1988 г. был разработан адаптивный алгоритм конструктивной теоремы об остатках. В последующем это направление активно развивалось и доведено в настоящее время до практического использования при передаче телеметрической информации (ТМИ) по космическим радиоканалам. Помимо универсального алгоритма разработаны ряд частных алгоритмов, работающих под его управлением и предназначенных для повышения достоверности информации, принимаемой в условиях помех различного происхождения. Показано, что результаты восстановления с использованием универсального алгоритма не имеют отличий от данных, получаемых при использовании известных теорем об остатках, но отличаются простотой технической реализации и более высоким уровнем приспособления к различным областям технического применения.

Его использование позволяет обеспечить возможность глубокого распараллеливания процесса восстановления значения X на основе остатков b_i путем последовательного задания двух модулей сравнения, условно обозначенных, как m_1 и m_2 [12–19]

$$X=\begin{cases} m_1\cdot\Delta/n+b_1, \quad \Delta=b_1-b_2\ge 0, (m_1<m_2); \\ m_1\cdot(m_2+\Delta/n)+b_1, \quad \Delta<0, n\mid\Delta; \\ m_1\cdot(m_2+\Delta)/n+b_1, \quad \Delta<0, \Delta>0, \\ \qquad n\mid\Delta, n\div\Delta, n\mid(m_2+\Delta); \\ m_1\cdot\left[m_2-(m_2-\Delta)\right]/n+b_1, \quad \Delta<0, \Delta>0, \\ \qquad n\mid\Delta, n\div\Delta, n\mid(m_2-\Delta); \\ m_1\cdot(2\cdot m_2+\Delta)/n+b_1, \quad \Delta<0, \Delta>0, \\ \qquad n\mid\Delta, n\div\Delta, n\mid(2\cdot m_2+\Delta); \\ m_1\cdot\left[m_2-(2\cdot m_2-\Delta)/n\right]+b_1, \quad \Delta<0, \Delta>0, \\ \qquad n\mid\Delta, n\div\Delta, n\mid(2\cdot m_2-\Delta); \\ \ldots \\ m_1\cdot(k\cdot m_2+\Delta)/n+b_1, \quad \Delta<0, \Delta>0, \\ \qquad n\mid\Delta, n\div\Delta, n\mid(k\cdot m_2+\Delta); \\ m_1\cdot\left[m_2-(k\cdot m_2-\Delta)/n\right]+b_1, \quad \Delta<0, \Delta>0, \\ \qquad n\mid\Delta, n\div\Delta, n\mid(k\cdot m_2-\Delta), \end{cases} \tag{4}$$

где $n=|m_1-m_2|$ – абсолютная разность между модулями сравнения m_1 и m_2;

$\Delta=b_1-b_2$ – представляет собой значения разности между образами-остатками $b_i(\mathrm{mod}\ m_i)$ и $b_j(\mathrm{mod}\ m_j)$, $(m_1<m_2)$, а обозначения $n\div\Delta$, $n\mid(k\cdot m_2+\Delta)$, $n\mid(k\cdot m_2-\Delta)$, $k=0,1,...$ читаются как: Δ не делится на n без остатка (знак отсутствия делимости «÷» и $k\cdot m_2+\Delta$, $k\cdot m_2-\Delta$ делятся на n без остатка (знак делимости «|»), при этом оперативность обратного восстановления тем выше, чем меньше n, а число используемых при этом параллельных звеньев алгоритма (4) равно $n+1$. Поэтому алгоритм ККТО является адаптивным, поскольку число параллельных звеньев восстановления X определяется разностью между модулями сравнения $n=|m_i-m_j|$. Следовательно, существует оптимальный набор модулей сравнения, при котором объем вычислений $O(q)\to\min$.

Пример. Предположим, что требуется найти X, удовлетворяющее системе сравнений

$$X\equiv b_1\ (\mathrm{mod}\ m_1);\ X\equiv b_2\ (\mathrm{mod}\ m_2);\ X\equiv b_3\ (\mathrm{mod}\ m_3) \tag{5}$$

при следующих значениях модулей сравнения $m_1=7$, $m_2=11$, $m_3=13$ и остатках $b_1=1$, $b_2=6$, $b_3=5$.

Решение. Используя второе формализованное представление китайской теоремы об остатках, получаем

1) $M_1=m_2\times m_3=143$, $143\times M_1'\equiv 1(\mathrm{mod}7)$, $M_1'=5$;
2) $M_2=m_1\times m_3=91$, $91\times M_2'\equiv 1(\mathrm{mod}11)$, $M_2'=4$;
3) $M_3=m_1\times m_2=77$, $77\times M_3'\equiv 1(\mathrm{mod}13)$, $M_2'=12$;

$x=143\times 5+91\times 4\times 6+77\times 12\times 5=7519\equiv 512(\mathrm{mod}1001)$.

Первая форма аналитического представления китайской теоремы об остатках приводит к следующей вычислительной процедуре:

$$X=b_1\times M_1^{\varphi(m_1)}+b_2\times M_2^{\varphi(m_2)}+b_3\times M_3^{\varphi(m_3)}\ (\mathrm{mod}\ m_1m_2m_3).$$

Функция Эйлера $\varphi(m_i)$ простого числа $m_i=p$ равна $\varphi(p)=p-1$. Следовательно,

$$X=143^6+6\times 91^{10}+5\times 77^{12}\equiv 512(\mathrm{mod}1001).$$

Нахождение значения X по теореме Х.Л. Гарнера предполагает определение мультипликативно-обратных элементов C_{ij}

$C_{12}\times 7\equiv 1(\mathrm{mod}11)\Rightarrow C_{12}=8$;
$C_{13}\times 7\equiv 1(\mathrm{mod}13)\Rightarrow C_{13}=2$;
$C_{23}\times 11\equiv 1(\mathrm{mod}13)\Rightarrow C_{23}=6$

и вычисление коэффициентов v

$v_1=1$, $v_2=(6-1)\times 8\equiv 7(\mathrm{mod}11)$;
$v_3=[(5-1)\times 2-7]\times 6\equiv 6(\mathrm{mod}13)$.

Тогда

$$X=v_3\times m_2\times m_1+v_2\times m_1+v_1=6\times 11\times 7+7\times 7+1=512.$$

Использование теоремы Х.Л. Гарнера приводит к уменьшению алгоритмической сложности процедуры нахождения X, поскольку мультипликативно-обратные элементы определяются по небольшим (по абсолютной величине) модулям сравнения (m_i, а не по M/m_i, где $M=\prod_{i=1}^{k} m_i$). При этом операции сравнения по модулям m_i производятся только при вычислении коэффициентов v.

В соответствии с предлагаемой конструктивной китайской теоремой об остатках исходную систему сравнений представим в виде следующих двух систем сравнений:

$$\begin{cases} X=1\ (\mathrm{mod}\ 7); \\ X=6\ (\mathrm{mod}\ 11); \\ X=5\ (\mathrm{mod}\ 13); \end{cases} \Rightarrow (6) \quad \begin{cases} X=1\ (\mathrm{mod}\ 7); \\ X=6\ (\mathrm{mod}\ 7); \\ \mathbf{X=1\ (mod\ 7)}; \\ \mathbf{X=5\ (mod\ 13)}. \end{cases} \tag{7}$$

Далее для каждой из полученных систем сравнений определяют следующие исходные данные: $\Delta=b_i-b_j$, $i<j$; $n=|m_i-m_j|$, необходимые для установления типа делимости без $n\mid(k\cdot m_{ij}+\Delta)$ или $n\mid(k\cdot m_{ij}-\Delta)$ при наименьшем $k=0,1,2,...$ Значением k и типом делимости определяется выбор соответствующего звена $2k-1$ или $2k-2$ формулы (2) для нахождения искомого значения X.

Для первой системы сравнений (6) с модулями $m_1=7$ и $m_2=11$, $\Delta=-5$, $n=4$, $n\mid(k\cdot m_{ij}-\Delta)$, $k=1$. Это приводит к следующему алгоритму восстановления:

$X^{(1)}=7\times(11-(11+5)/4)+1=50$

и $X^{(2)}=11\times(7-(7+5)/4)+6=50$.

Для второй системы сравнений (7) с модулями m_1=7 и m_2=13 соответствующие исходные данные равны Δ=–4, n=6, $n|(k\cdot m_{ij}-\Delta)$, k=2. Следовательно,

$X^{(1)}$=7×(13–(26+4)/6)+1=57

и $X^{(2)}$=13×(7–(14+4)/6)+5=57.

Совпадение двух полученных результатов $X^{(1)}$ и $X^{(2)}$ обеспечивает возможность контроля достоверности восстановления и свидетельствует о том, что восстановление произведено верно.

Следующий этап восстановления методом «подъема значений модулей сравнения» предполагает переход к системе из двух сравнений, эквивалентной исходной, но с укрупненными модулями

$$\begin{cases} x = 50 \pmod{7\times 11}; \\ x = 57 \pmod{7\times 13}. \end{cases} \qquad (8)$$

Определяем исходные данные Δ=50–57=–7, n=91–77=14, $n|(k\cdot m_{ij}-\Delta)$, k=1,2 в соответствии с установленным типом делимости восстанавливаем X

$$X = 77\times\left(\frac{91-7}{14}\right)+50 = 91\times\left(\frac{77-7}{14}\right)+57 = 512.$$

Полученный результат не имеет отличий от результатов восстановления, полученных с использованием других теорем об остатках.

При этом решение системы сравнения (7) не может быть получено при использовании известных классических алгоритмов теорем об остатках, так как не выполняется условие взаимной простоты укрупненных модулей сравнении (m_i, m_j)=1. У них есть делитель – число 7, которое отличается от 1.

Если производится сравнение по составным модулям $M_1=p\cdot m_1$ и $M_2=p\cdot m_2$, то справедливы следующие записи:

$$\begin{cases} X \equiv b_1 \pmod{m_1}; \\ X \equiv b_2 \pmod{m_2}; \end{cases} \Rightarrow \begin{cases} X \equiv p\cdot b_1 \pmod{p\cdot m_1}; \\ X \equiv p\cdot b_2 \pmod{p\cdot m_2}. \end{cases} \qquad (9)$$

Исходные данные, необходимые для восстановления в соответствии с алгоритмом ККТО

$n^*=|M_1-M_2|=p\cdot|m_1-m_2|=p\cdot n$

и $\Delta^*=p\cdot b_1-p\cdot b_2=p\cdot(b_1-b_2)\ p\cdot\Delta$.

Тогда $p\cdot\Delta/p\cdot n=\Delta/n$ и, следовательно, обеспечивается однозначность восстановления X при составных модулях.

Эта особенность имеет важное значение для расширения области применения *конструктивной теории конечных полей* [12–19], основу которой составляет ККТО. В этом случае снимается жесткое ограничение классической теории полей Э.Галуа на выбор модулей сравнения в виде чисел и полиномов [2–5].

Представленные выше формы аналитического описания *китайской теоремы об остатках* относятся к так называемой «модулярной арифметике», когда модули сравнения представлены целыми числами.

Но наибольшую прикладную значимость в современной информатике получили алгоритмы *китайской теоремы об остатках* «полиномиальной арифметики», когда модулями являются полиномы (многочлены). Они составляют основу современной алгебраической теории помехоустойчивого кодирования [8 - 10] и цифровой обработки сигналов [6].

3. Обоснование вида закона распределения статистических данных при их представлении образами-остатками

Распространение изложенных выше теоретических выводов в области статистического анализа экспериментальных данных приводит к необходимости исследовать вопросы обоснования вида закона распределения статистических данных при их представлении образами–остатками, что целесообразно начать с нормального закона распределения, имеющего наиболее широкое распространение.

Представление статистических данных, имеющих нормальный вид закона распределения, по модулям сравнения приводит к трансформации исходной плотности распределения вероятностей. Так, например, при выборе модулей сравнения из условия $m\approx 3\sigma_x$ ось абсцисс будет представлена конечными остатками от деления при представлении её по модулю сравнения, а плотность распределения вероятностей можно представить в виде суммы

$$\varphi_m(x) = \sum_{i=-\infty}^{\infty} \varphi(x-\delta-i\cdot m), \qquad (10)$$

где δ – величина сдвига начала интервала интегрирования от математического ожидания по модулю сравнения m.

Без большого ущерба в точности получаемых вычислений можно принять $\varphi(x)\approx 0$ при $x\geq 3\sigma_x$ или $x\leq -3\sigma_x$, что позволяет представить равенство (9) в упрощенном виде

$$\varphi_m(x)\approx\varphi(x-\delta)+\varphi(x-\delta+3\sigma_x)+ +\varphi(x-\delta+6\sigma_x). \qquad (11)$$

Следует отметить, что в этом случае

$$\varphi_m\ x = \begin{cases} 0, & при \quad x<0; \\ \sum\limits_{i=-\infty}^{\infty} \varphi\ x-\delta-i\cdot m\ , & при \quad 0\leq x<3\sigma_x; \\ 0, & при \quad x\geq 3\sigma_x, \end{cases} \qquad (12)$$

поскольку все случайные величины укладываются в интервал $0 \le x < 3\sigma_x$.

Результирующая плотность распределения $\varphi_m(x)$ в соотношении (11) может быть определена с использованием характеристических функций, когда

$$g(\lambda) = \int_{-\infty}^{\infty} \exp\{i\lambda x\} \cdot \frac{1}{\sigma_x\sqrt{2\pi}} \cdot \exp\left\{-\frac{(x-m_x)^2}{2\sigma_x^2}\right\} dx =$$

$$= \frac{1}{\sigma_x\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left\{-\frac{x^2 - 2xm_x + m_x^2}{2\sigma_x^2} + i\lambda x\right\} dx =$$

$$= \frac{1}{\sigma_x\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left\{-\frac{1}{2\sigma_x^2} \cdot x^2 + \left(\frac{m_x}{\sigma_x^2} + i\lambda\right) \cdot x - \frac{m_x^2}{2\sigma_x^2}\right\} dx \cdot$$

Опираясь на известное правило интегрирования

$$\int_{-\infty}^{\infty} \exp\{-A \cdot x^2 \pm B \cdot x - C\} dx = \sqrt{\frac{\pi}{A}} \cdot \exp\left\{-\frac{AC - B^2}{A}\right\},$$

можно, опуская промежуточные выкладки, записать

$$g(\lambda) = \exp\left\{-\frac{1}{2}\sigma_x^2\lambda^2 + im_x\lambda\right\}.$$

Это общее уравнение удобно использовать для записи характеристических функций слагаемых в (11), когда

$$m_{x1} = m_x + \delta \Rightarrow g_1(\lambda) = \exp\left\{-\frac{1}{2}\sigma_x^2\lambda^2 + i(m_x + \delta)\lambda\right\};$$

$$m_{x2} = m_x - 3\sigma_x + \delta \Rightarrow g_2(\lambda) =$$

$$= \exp\left\{-\frac{1}{2}\sigma_x^2\lambda^2 + i(m_x - 3\sigma_x + \delta)\lambda\right\};$$

$$m_{x3} = m_x - 6\sigma_x + \delta \Rightarrow g_3(\lambda) =$$

$$= \exp\left\{-\frac{1}{2}\sigma_x^2\lambda^2 + i(m_x - 6\sigma_x + \delta)\lambda\right\}.$$

Соответственно, характеристическая функция результирующей плотности вероятностей будет иметь следующий вид:

$$\tilde{g}(\lambda) = g_1(\lambda) \cdot g_2(\lambda) \cdot g_3(\lambda) =$$

$$= \exp\left\{-\frac{3}{2}\sigma_x^2\lambda^2 + 3i(m_x - 3\sigma_x + \delta)\lambda\right\}. \quad (13)$$

В дальнейшем, полагая

$$\tilde{\sigma}_x = 3\sigma_x \text{ и } \tilde{m}_x = 3(m_x - 3\sigma_x + \delta),$$

характеристическая функция (12) примет вид

$$\tilde{g}(\lambda) = \exp\left\{-\frac{1}{2}\tilde{\sigma}_x^2\lambda^2 + i\tilde{m}_x\lambda\right\},$$

что соответствует плотности распределения

$$\tilde{\varphi}_m(x) = \begin{cases} 0, & при \quad x < 0; \\ \dfrac{1}{\tilde{\sigma}_x\sqrt{2\pi}} \cdot \exp\left\{-\dfrac{(x-\tilde{m}_x)^2}{2\tilde{\sigma}_x^2}\right\}, & \\ & при \quad 0 \le x < 3\sigma_x; \\ 0, & при \quad x \ge 3\sigma_x. \end{cases} \quad (14)$$

В более общем случае, когда модуль сравнения не является кратным $3\sigma_x$ полученные зависимости (12)–(14) можно записать следующим образом:

• исходное представление результирующей плотности распределения вероятностей

$$\varphi_m(x) = \begin{cases} 0, & при \quad x < 0; \\ \sum\limits_{i=-\infty}^{\infty} \varphi(x - \delta - i \cdot m), & при \quad 0 \le x < m; \\ 0, & при \quad x \ge m; \end{cases} \quad (15)$$

• характеристическая функция результирующей плотности распределения вероятностей

$$\tilde{g}(\lambda) = \exp\left\{-\frac{N}{2}\sigma_x^2\lambda^2 + iN\left(m_x - \frac{N-1}{2} \cdot m + \delta\right)\lambda\right\}, \quad (16)$$

где количество членов суммирования N выбирается из условия

$$N \cdot m \ge 3\sigma_x \Rightarrow N \ge \frac{3}{m}\sigma_x;$$

• результирующая плотность распределения вероятностей

$$\tilde{\varphi}_m(x) = \begin{cases} 0, & при \quad x < 0; \\ \dfrac{1}{\tilde{\sigma}_x\sqrt{2\pi}} \cdot \exp\left\{-\dfrac{(x-\tilde{m}_x)^2}{2\tilde{\sigma}_x^2}\right\}, & \\ & при \quad 0 \le x < m; \\ 0, & при \quad x \ge m, \end{cases} \quad (17)$$

где $\tilde{\sigma}_x = N \cdot \sigma_x$ и $\tilde{m}_x = N\left(m_x - \dfrac{N-1}{2}\sigma_x + \delta\right)$.

Полученный результат (14), (17) представляет интерес в том смысле, что плотность распределения вероятностей случайных величин, представимых по модулям сравнения, отличается большей пологостью ($\tilde{\sigma}_x = N \cdot \sigma_x$) и этот факт становится значимым при решении многих прикладных задач, поскольку позволяет существенным образом упростить расчёт интегралов вероятностей. Так, для малых интервалов интегрирования при $\Delta x < \sigma_x$ расчёт интегралов вероятностей с приемлемой точностью можно выполнять по методу прямоугольников или трапеций.

Литература

1. Диффи У., Хелман М. Защищенность и имитостойкость: / Введение в криптографию // ТИИЭР, том 67, №3, 1979.
2. Кнут Д. Искусство программирования для ЭВМ т.2, Получисленные алгоритмы. - М.: Мир, 1977. – 724с.

3. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х томах. Пер с англ. - М.: Мир, 1988. – 882с.
4. Макклеллан Дж., Рейдер Ч. Применение теории чисел в цифровой обработке сигналов/ Пер. с анг.- М. Радио и связь. 1983. – 376с.
5. Свердлик М.Б. Оптимальные дискретные сигналы. - М.: Сов. Радио, 1975. – 200с.
6. Блейхут Р. Теория и практика кодов, контролирующих ошибки. - М.: Мир, 1986. –576с.
7. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. / Пер. с англ. – М.: Связь, 1979. – 744с.
8. Кларк Дж., Мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. / Пер. с англ. – М.: Радио и связь, 1987. – 392с.
9. Стахов А.П. Введение в алгоритмическую теорию измерения.-М.: Сов.радио, 1973. – 120с.
10. Фомин С.В. Системы счисления. М.: Наука. Главная редакция физико-математической литературы, 1980. – 48с.
11. Космические траекторные измерения. Радиотехнические методы измерений и математическая обработка данных /Под ред. Агаджанова П.А., Дулевича В.Е., Коростелева А.А/ -М.: Сов. радио, 1969. - 504с.
12. Калашников И.Д., Степанов В.С., Чуркин А.В. Адаптивные системы сбора и передачи информации. - М.: Энергия, 1975. – 240с.
13. Адаптивные телеизмерительные системы: Под ред. А.В.Фремке. - Л.: Энергоиздат, 1981. –248с.
14. Ольховский Ю.Б., Новоселов О.Н., Мановцев А.П. Сжатие данных при телеизмерениях. – М.: Сов. радио, 1971.– 278с.
15. Торгашев В.А. Система остаточных классов и надежность ЦВМ. - М.: Сов. радио, 1973. – 120с.
16. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. - М.: Сов. Радио, 1968. – 140с.
17. Цифровые методы в космической связи/ Пер. с англ.,// Под редакцией С Голомба. – М.: Связь, 1969. – 266с.
18. Зюко А.Г. Помехоустойчивость и эффективность систем связи. - М.: Связь, 1972. – 360с.
19. Информационные технологии в радиотехнических системах /Под ред. И.Б.Федорова/. – М.: Изд. МГТУ имени Н.Э.Баумана, 2003 – 672с.
20. ГЛОНАСС. Принципы построения и функционирования /Под ред. А.И.Перова, В.Н.Харисова. изд. 4-е, перераб. И доп. –М.: Радиотехника, 2010 – 800с.
21. И.М.Тепляков Радиотелеметрия. – М.: «Сов. радио», 1966. – 311с.
22. Былински П., Ингрем Д. Цифровые системы передачи: Пер. с анг./Под ред. А.А.Визеля. – М.: Связь, 1980. – 360с.
23. Шумоподобные сигналы в системах передачи информации /Под ред. проф. В.Б.Пестрякова. – М.: «Сов. радио», 1973.- 424с.
24. «Современная телеметрия в теории и на практике / Учебный курс», Спб.: Наука и Техника, 2007. – с. 672.
25. Кукушкин С.С. Теория конечных полей и информатика: том.1 Методы и алгоритмы, классические и нетрадиционные, основанные на использовании конструктивной теоремы об остатках – М: МО РФ, 2003. – 281с.
26. Кукушкин С.С. Методы анализа и синтеза различных проблемно-ориентированных подходов к устранению избыточности передаваемой информации, «Двойные технологии»/, М.: СИП РИА, №2, 2010 – с. 9 –13.
27. Кукушкин С.С. Методы конструктивной теории синтеза нетрадиционных представлений данных и сигналов для повышения эффективности передачи информации, «Двойные технологии», М.: СИП РИА, №3, 2010 – с. 13–17.

Материал поступил в редакцию 08. 02. 2014 г.