УДК 621.396

© Кукушкин С.С., Войналович В.В., Половников А.Ю.
Kukushkin S.S. Voinalovich V.V., Polovnikov A.J.

МЕТОД СИНТЕЗА ПРОБЛЕМООРИЕНТИРОВАННОГО КОДА ДЛЯ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ ПЕРЕДАЧИ ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ

METHOD OF THE SYNTHESES PROBLEMOORIENTIROVANNOGO CODE FOR INCREASING OF NOISE-IMMUNITY OF THE TRANSMISSION TO MEASURING INFORMATION

Аннотация. *В статье рассматривается задача синтеза кода, адаптированного для повышения помехоустойчивости передачи измерительной информации. Для решения данной задачи предлагается использовать такой мощный и хорошо разработанный аналитический аппарат, как теория конечных полей.*

Annotation. *In article is considered task of the syntheses of the code, adapted for increasing of noise-immunity of the transmission to measuring information. For decision given tasks is offered use such powerful and well designed analytical device, as theory by final flap.*

Ключевые слова. *Помехоустойчивость, передача измерительной информации, теория конечных полей.*

Key words. *Noise-immunity, issue to measuring information, theory by final flap.*

1. Актуальность решаемой задачи

Одной из основных проблем, возникающих при передаче измерительной информации, является уменьшение погрешности измерений и противостояние разрушающему действию помех и шумов при их передаче по каналам связи.

В данной статье рассматривается задача синтеза кодов, адаптированных для повышения помехоустойчивости передачи измерительной информации. Для решения данной задачи предлагается использовать такой мощный и хорошо разработанный аналитический аппарат как теория конечных полей [1, 2].

2. Применение ортогональных матриц Адамара

В настоящее время результаты измерений подвергаются определенным преобразованиям, имеющим основной целью повышение помехоустойчивости их передачи по каналам с шумами. Это достигается за счет введения определенной структурной взаимосвязи между измерениями. Чаще всего она выражается в алгебраической форме, представляющей собой систему линейных уравнений. Замена их эквивалентными системами сравнений составляет основу нового подхода к синтезу оптимального плана преобразований результатов измерений и помехоустойчивого кодирования передаваемой информации. Рассмотрим основные положения такого подхода к планированию измерительного эксперимента и оптимальному формированию его результатов на основе теории конечных полей и конструктивной теоремы об остатках [2].

Одно из направлений синтеза оптимального плана преобразований (кода) результатов измерений связано с использованием ортогональных матриц Адамара, которые составляют основу синтеза оптимальных помехоустойчивых кодов, известных под названием кодов

Кукушкин Сергей Сергеевич – доктор технических наук, профессор, ведущий научный сотрудник 4 ЦНИИ Минобороны России, тел. 515-19-82,
Войналович Владимир Владимирович – кандидат технических наук, старший научный сотрудник 4 ЦНИИ Минобороны России, тел.+7(495)502-84-23;
Половников Алексей Юрьевич – кандидат технических наук, старший научный сотрудник, заместитель начальника управления 4 ЦНИИ Минобороны России, тел. +7(495)502-84-23.

Kukuschkin Sergej Sergeevich – Dr. Sci. Tech., the professor conducting the scientific employee, 4 CNII the Ministries of Defense, tel. 515-19-82,
Voinalovich Vladimir Vladimirovich – Ph., the senior scientific employee 4 Central Scientific Research Institute Ministry of Defence of Russia., tel. +7(495)502-84-23;
Polovnikov Aleksey Jurievich – Ph., the senior scientific employee, the deputy chief of department 4 Central Scientific Research Institute Ministry of Defence of Russia, the senior scientific employee, tel. +7(495)502-84-23.

Плоткина [3-5]. Матрицами Адамара определяются и наилучшие весовые планы, создающие основу для уменьшения систематической и случайной ошибки измерений. Матрицы Адамара представляют собой математическую модель формирования оптимальной структуры представления результатов измерений. Понятие оптимальности связано с возможностью достижения теоретической границы помехоустойчивости, известной как граница Плоткина.

Их суть заключается в следующем. Предположим для определенности, что имеют место измерения *a, b, c* и *d*. Их необходимо передать с объекта контроля по каналу связи, подверженному действию помех, результатами действия которых являются погрешности измерений $\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4$, принадлежащие плотностям распределения вероятности ошибок с нулевым средним и дисперсией σ^2: $a^* = a + \varepsilon_1$, $b^* = b + \varepsilon_2$, $c^* = c + \varepsilon_3$, $d^* = d + \varepsilon_4$.

Основу преобразований результатов измерений могут составить матрицы Адамара, являющиеся ортогональными матрицами размерности $n \times n$, элементами которой являются действительные числа +1 и –1, например,

$$H_2 = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix}.$$

Оптимальный в смысле границы Плоткина план измерений (схема кодирования) заключается в том, чтобы операции суммирования и вычитания полученных результатов выполнить в соответствии с матрицей Адамара. Для рассмотренных четырех результатов измерений *a, b, c* и *d* это матрица H_4. Следовательно, получим следующие четыре уравнения:

$$\begin{aligned} a + b + c + d &= y_1; \\ a - b + c - d &= y_2; \\ a + b - c - d &= y_3; \\ a - b - c + d &= y_4. \end{aligned} \qquad (1)$$

Полученные значения y_1, y_2, y_3, y_4 и есть либо так называемые косвенные измерения для случая планирования измерительного эксперимента, либо результат помехоустойчивого кодирования при передаче по каналам связи с помехами. Измерения y_1, y_2, y_3, y_4 также характеризуются относительными погрешностями измерений (ошибками) ε_i, принадлежащие плотностям распределения вероятности ошибок с нулевым средним и дисперсией

σ^2: $y_1^* = y_1 + \varepsilon_1$, $y_2^* = y_2 + \varepsilon_2, y_3^* = y_3 + \varepsilon_3, y_4^* = y_4 + \varepsilon_4$.

Операция извлечения интересующих значений измерений (декодирования) связана с определением следующих оценок:

$$a^* = (y_1 + y_2 + y_3 + y_4)/4 + (\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4)/4.$$

Следовательно, дисперсия погрешности (шума) измерения a^* будет равна: $\sigma^2/4$. Это означает, что будет обеспечен выигрыш, соответствующий порядку матрицы Адамара. Аналогичный результат будет получен и при восстановлении других измерений.

В общем случае, когда существует матрица Адамара порядка n, то рассмотренное кодирование уменьшает дисперсию шума (погрешности измерений) в *n* раз: σ^2/n. Однако достигается этот положительный эффект соответствующим увеличением избыточности передаваемых символов помехоустойчивого кода (расширением шкалы представления данных при измерениях).

С точки зрения обеспечения требуемого уменьшения дисперсии шума (погрешности измерений) при наименьшей избыточности передаваемой информации (шкалы представления) используют данные y_i, принимающие только положительные значения. Вычеркивая первую строку и последний столбец (1) с заменой в соответствующих уравнениях, связывающих измерения *a, b, c, d* коэффициента «–1» на коэффициент «0» получаем

$$\begin{aligned} a \quad + c &= y_1; \\ a + b \quad &= y_2; \\ a \quad &= y_3. \end{aligned}$$

В этом случае оценка результата измерений (декодированного сообщения) a^* определяется следующим аналитическим представлением:

$$a^* = (y_1 - y_2 + y_3)/4 - (\varepsilon_1 - \varepsilon_2 + \varepsilon_3)/4 =$$
$$= a - (\varepsilon_1 - \varepsilon_2 + \varepsilon_3)/4.$$

В общем случае, если существует матрица Адамара порядка *n*, то данный способ кодирования позволяет уменьшить дисперсию погрешности (шума) до $4n\sigma^2/(n+1)^2$. Выигрыш не столь значительный по сравнению с ранее рассмотренным случаем. Но в качестве компенсации проигрыша появляется возможность уменьшения в $(n + 1)/2$ раз систематической ошибки измерений. Кроме того, упрощается операция кодирования и уменьшается число избыточных символов.

3. Применение конструктивной теоремы об остатках

Замена линейных уравнений эквивалентными системами сравнений и использование конструктивной теоремы об остатках позволяет достичь более высокого положительного эффекта.

$$\begin{aligned} a \quad + c \quad &= y_{11} (mod\ m_1); \\ a + b \quad &= y_{12} (mod\ m_1); \\ a \quad &= y_{13} (mod\ m_1). \end{aligned}$$

$$\begin{aligned} a \quad + c \quad &= y_{21} (mod\ m_2); \\ a + b \quad &= y_{22} (mod\ m_2); \\ a \quad &= y_{23} (mod\ m_2). \end{aligned}$$

В качестве подтверждения возможности достижения качественно более высокого положительного эффекта при использовании гомоморфных образов измерений рассмотрим следующий пример. Предположим, что в случае традиционного представления результаты измерений имели значения a=116, b=97, c=218, d=43.

Преобразование измерительной информации, ориентированное на использование в качестве исходных данных образов измерений, приводит к увеличению вдвое размерности матрицы Адамара по сравнению с традиционным правилом ее применения.

Для данного примера кодирование гомоморфных образов измерений предполагает использование матриц Адамара H_8 вместо H_4 для случая традиционного представления данных.

Результаты измерений, представленные гомоморфными образами

Измерение	116		97		218		43	
Модуль	m_1=15	m_2=17	m_1=15	m_2=17	m_1=15	m_2=17	m_1=15	m_2=17
Образ	a_1=11	b_1=14	c_1=7	d_1=12	e_1=8	f_1=14	g_1=13	h_1=9

Кодирование осуществляется на основе суммирования остатков по схеме, определяемой матрицей Адамара H_8 и приводящей к следующей системе уравнений:

$y_{11} = a_1 + c_1 + e_1 + g_1 = 11 + 7 + 8 + 13 = 39;$
$y_{12} = b_1 + c_1 + f_1 + g_1 = 14 + 7 + 14 + 13 = 48;$
$y_{13} = a_1 + b_1 + e_1 + f_1 = 11 + 14 + 8 + 14 = 47;$
$y_{14} = d_1 + e_1 + f_1 + g_1 = 12 + 8 + 14 + 13 = 47;$
$y_{15} = a_1 + c_1 + d_1 + f_1 = 11 + 7 + 12 + 14 = 44;$
$y_{16} = b_1 + c_1 + d_1 + e_1 = 14 + 7 + 12 + 8 = 41;$
$y_{17} = a_1 + b_1 + d_1 + g_1 = 11 + 14 + 12 + 13 = 50.$

Избыточность символов сформированных сообщений составляет 50%. Следовательно, в 1,5 раза увеличится объем передаваемой информации, а дисперсия шума уменьшится в 2,3 раза.

Предположим, что кроме шумовой присутствует и систематическая составляющая погрешности измерений. В результате, например, вместо рассмотренной последовательности данных измерений: {39, 48, 47, 47, 44, 41, 50} принята последовательность {44, 53, 52, 52, 49, 46, 55}. В этом случае при декодировании на основе обратной матрицы Адамара H_8^* ($H_8^* + H_8 = 0$)

$$H_8^* = \begin{vmatrix} - & - & - & - & - & - & - & - \\ - & 1 & - & 1 & - & 1 & - & 1 \\ - & - & 1 & 1 & - & - & 1 & 1 \\ - & 1 & 1 & - & - & 1 & 1 & - \\ - & - & - & - & 1 & 1 & 1 & 1 \\ - & 1 & - & 1 & 1 & - & 1 & - \\ - & - & 1 & 1 & 1 & 1 & - & - \\ - & 1 & 1 & - & 1 & - & - & 1 \end{vmatrix}$$

будут получены следующие оценки гомоморфных образов измерений (остатков):

$a_1^* = (\ 44 - 53 + 52 - 52 + 49 - 46 + 55)/4 = 12,25;$
$b_1^* = (-44 + 53 + 52 - 52 - 49 + 46 + 55)/4 = 15,25;$
$c_1^* = (\ 44 + 53 - 52 - 52 + 49 + 46 - 55)/4 = 8,25;$
$d_1^* = (-44 - 53 - 52 + 52 + 49 + 46 + 55)/4 = 13,25;$
$e_1^* = (\ 44 - 53 + 52 + 52 - 49 + 46 - 55)/4 = 9,25;$
$f_1^* = (-44 + 53 + 52 + 52 + 49 - 46 - 55)/4 = 15,25;$
$g_1^* = (\ 44 + 53 - 52 + 52 - 49 - 46 + 55)/4 = 14,25.$

Так как передаче подлежат только целочисленные значения, то округление результатов до ближайшего целого числа приведет к получению следующих оценок образов (остатков) измерений: {12, 15, 8, 13, 9, 15, 14}. Последующее декодирование с использованием алгоритма конструктивной теоремы об остатках приведет к получению следующих результатов:

$1) \Delta_{12} = 12 - 15 = 3; \quad n = |m_1 - m_2| = 2;$

$$k=1 \Rightarrow x_1 = 15 \cdot \frac{17-3}{2} + 12 = 17 \cdot \frac{15-3}{2} + 15 = 117.$$

Аналогичным образом находим

$2)\ x_2 = 98;$
$3)\ x_3 = 219;$
$4)\ x_4 = 44.$

Сравнение с исходными данными, приведенными в таблице, показывает, что систематическая составляющая ошибки восстановленных результатов измерений уменьшена в 5 раз. Вместе с тем будет уменьшена и случайная составляющая погрешности измерений. Дисперсия и среднеквадратическое отклонение погрешностей восстановления переданных сообщений-остатков будут равны

$$\sigma_{\text{п}}^2(\varepsilon) = \frac{4n\sigma^2(\varepsilon)}{(n+1)^2} = 0,4\sigma^2(\varepsilon); \qquad \sigma_{\text{п}}(\varepsilon) = 0,63\sigma(\varepsilon).$$

Это означает, что в сравнении с традиционной передачей погрешность восстановления результатов измерений будет уменьшена в 1,6 раза. Новизна предлагаемого решения заключена в применении математического аппарата преобразования (кодирования) данных на основе матриц Адамара не к непосредственным результатам измерений, а к их остаткам. Необходимо отметить, что наиболее часто результат измерения в традиционной форме получить сложнее, чем при представлении системой образов. Это имеет место, например, при косвенных измерениях, а также в случае многошкальных измерений.

Поэтому отображение измерений образами является более естественной формой представления измерительной информации.

4. Заключение

Использование матриц Адамара тем эффективнее, чем больше ее порядок n. Когда же мы переходим от элементов, представленных в традиционном виде, к элементам, которые являются их образами-остатками, то в два раза повышается порядок матриц Адамара. При этом в 5 раз уменьшается систематическая ошибка по сравнению с традиционным представлением данных и в 9 раз уменьшаются шумы, искажающие образы-остатки при их передаче по радиоканалам с ограниченной пропускной способностью.

Необходимо отметить, что предлагаемый переход от исходных данных (сообщений) к их образам-остаткам, а также матричное представление последних составляют научно-методическую базу нового подхода к структурно-алгоритмической защите информации от НСД. Этот новый положительный эффект связан не только с затруднением доступа к смысловому содержанию информации, но и с повышением помехоустойчивости передаваемых сообщений. Основу достижения положительного комплексного эффекта составляет реконструкция традиционной позиционной системы счисления. Ее основной недостаток состоит в том, что вклад искаженного двоичного символа в ошибку результата измерений стремительно растет от младшего разряда к старшему. Вклад самого младшего разряда равен: $2^0 = 1$, а самого старшего (восьмого разряда при байтовом представлении слов) $2^7 = 128$. Помеха с равной вероятностью может исказить и младший, и самый старший разряд [2]. Предлагаемое смешанное представление (позиционное внутри остатков и непозиционное из-за независимости восстанавливаемого результата от занимаемого места (позиции) полуслов-остатков в новом восьмиразрядном слове) этого недостатка в значительной степени лишено. Самый младший разряд полуслова-остатка имеет, по-прежнему, вес $2^0 = 1$, а его самый старший (четвертый разряд) – вес $2^3 = 8$. Поэтому новая конструкция информационных слов имеет в $k = 2^7 / 2^3 = 16$ раз большую помехоустойчивость по сравнению с традиционным представлением. Это позволяет синтезировать различные алгоритмы восстановления данных.

Применение конструктивной теоремы [2] по сравнению с аналогом – китайской теоремы об остатках также дает выигрыш в самом общем случае (при отсутствии свойств непрерывности (корреляционной зависимости) передаваемых значений в 1,3 раза.

Литература

1. Свердлик М.Б. Оптимальные дискретные сигналы.-М.:Сов. радио,1975.–200с.

2. Кукушкин С.С. Теория конечных полей и информатика: в 2-х томах, т.1. Методы и алгоритмы, классические и нетрадиционные, основанные на использовании конструктивной теоремы об остатках – М.: Минобороны России, 2000. – 237с.

3. Блейхут Р. Теория и практика кодов, контролирующих ошибки. -М.: Мир, 1986. – 576с.

4. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. / Пер. с англ.– М.: Связь, 1979. –744с.

5. Кларк Дж., мл., Клейн Дж. Кодирование с исправлением ошибок в системах цифровой связи./Пер. с англ.–М.:Радио и связь, 1987.–392с.

Материал поступил в редакцию12. 08. 2009 г.