ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ / PHYSICS AND MATHEMATICS

Научная статья
УДК 519.142.6:621.391
https://doi.org/10.35266/1999-7604-2024-3-10

Кодирование информации линейными перестановками дискретного преобразования Уолша

Михаил Сергеевич Беспалов[1], Кирилл Андреевич Фролов[2]✉
[1, 2]Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия
[1]bespalov@vlsu.ru, https://orcid.org/0000-0003-0661-337X
[2]golegoga33rus@gmail.com✉, https://orcid.org/0000-0001-8691-8151

Аннотация. В работе предложен метод использования кодовой матрицы в виде закрытого ключа для кода Уолша – Адамара. Посчитано число возможных кодовых матриц. Например, для матрицы Уолша порядка 32, то есть уровня 5, возможных ключей почти 10 миллионов. Показан способ декодирования информации и процедура выделения кодовой матрицы из зашифрованной матрицы Уолша.

Ключевые слова: линейный код, код Уолша – Адамара, дискретные преобразования Уолша, кодовая матрица, линейные перестановки

Для цитирования: Беспалов М. С., Фролов К. А. Кодирование информации линейными перестановками дискретного преобразования Уолша // Вестник кибернетики. 2024. Т. 23, № 3. С. 90–95. https://doi.org/10.35266/1999-7604-2024-3-10.

Original article

Information encoding by linear permutations of discrete Walsh transform

Mikhail S. Bespalov[1], Kirill A. Frolov[2]✉
[1, 2]Vladimir State University, Vladimir, Russia
[1]bespalov@vlsu.ru, https://orcid.org/0000-0003-0661-337X
[2]golegoga33rus@gmail.com✉, https://orcid.org/0000-0001-8691-8151

Abstract. The paper proposes a method for using a code matrix as a private key for the Walsh-Hadamard code. The number of possible code matrices has been calculated. For example, there are almost 10 million possible keys for a Walsh matrix of the order 32, they are also level 5. The paper describes the method of decoding information and the procedure for isolating the code matrix from the encrypted Walsh matrix.

Keywords: linear code, Walsh-Hadamard code, discrete Walsh transform, code matrix, linear permutations

For citation: Bespalov M. S., Frolov K. A. Information encoding by linear permutations of discrete Walsh transform. *Proceedings in Cybernetics*. 2024;23(3):90–95. https://doi.org/10.35266/1999-7604-2024-3-10.

ВВЕДЕНИЕ

При передаче сигналов по неустойчивому каналу связи используют метод кодирования с исправлением ошибок, который применяется для устранения ошибок замещения символа [1]. Рассмотрим линейные блоковые коды, известные как (n,k)-коды, где n – длина кодового слова, k – длина кодируемого сообщения. Подробное обозначение кода (n,k,d), где добавлен третий параметр d – кодовое расстояние, равное минимальному расстоянию Хэмминга между кодовыми словами [1].

Существует много работ, в которых приведено сравнение эффективности (n,k,d)-кодов [2, 3], подробно рассмотрена их классификация [4–6] и методы их декодирования [7].

При зашумленном канале (например, космическая связь) берут метод кодирования с максимально возможным d. К кодам такого типа относится код Уолша – Адамара, который служит линейным (2^k, k, 2^{k-1})-кодом. Для него разработаны и известны процедуры обнаружения и исправления ошибок.

Космическая связь служит открытым каналом связи. Поскольку результатами разработчиков могут воспользоваться конкурентные структуры, перехватившие передаваемый сигнал, то код Уолша – Адамара желательно совместить с элементами шифрования сигнала.

В статье предлагается дополнить этот код матричным методом кодирования в виде линейной перестановки дискретного преобразования Уолша, разработанной одним из авторов [8, 9].

МАТЕРИАЛЫ И МЕТОДЫ

Применение кода Уолша – Адамара при передаче информации

Множество кодовых слов кода Уолша – Адамара совпадает с множеством дискретных функций Уолша в аддитивной записи. Поясним понятие аддитивной записи.

Группу из двух элементов алгебраисты изучают: в аддитивной форме $\mathbb{Z}_2 = \{0,1; \oplus\}$ с операцией $\oplus$ сложения по модулю *2*; или в мультипликативной форме $\mathbb{Z}_2 = \{1, -1; \bullet\}$ с операцией умножения $\bullet$. К группе $\mathbb{Z}_2$ добавляется вторая операция, превращая ее в поле F_2. Множество n-мерных векторов с элементами из группы $\mathbb{Z}_2^n$ составляют n-мерное векторное пространство над полем F_2 с операциями $\oplus$ покоординатного сложения по модулю *2* (в аддитивном случае) или с операцией $\bullet$ умножения по Адамару (в мультипликативном случае). В аддитивном случае вторая внешняя операция есть операция умножения на элементы поля 0 или 1, что реализуется при составлении линейной комбинации векторов как включение вектора в сумму (при коэффициенте 1) или невключение (при коэффициенте 0). Аналогично составляются линейные комбинации и в мультипликативном случае, что позволяет специально не описывать вторую операцию. В этой терминологии можно предложить следующее алгебраическое описание дискретных функций Уолша.

Теорема 1. *Для $N = 2^n$ множество дискретных функций Уолша есть подмножество элементов мультипликативного представления векторного пространства $\mathbb{Z}_2^N$, изоморфное векторному пространству $\mathbb{Z}_2^n$.*

Все дискретные функции Уолша уровня n (порядка $N = 2^n$) записаны в строках матрицы Сильвестра – Адамара $H_n = H^{n\otimes}$, полученной в виде n-й кронекеровой [10] степени матрицы:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \qquad (1)$$

По этому определению получаем рекуррентную формулу вычисления матриц Сильвестра – Адамара [9]:

$$H_{n+1} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}. \qquad (2)$$

Линейное преобразование с матрицей H_n называется дискретным преобразованием Уолша (в нумерации Адамара) и встречается под аббревиатурой ДПУ (ДПУ – Адамара).

Проведя в H_n обратную перекодировку $1\to 0$, $-1\to 1$ из мультипликативной формы записи в аддитивную, в строках матрицы A_n получим все кодовые слова кода Уолша – Адамара соответствующего уровня. Например, при $k = 2$ кодовые слова в строках матрицы:

$$A_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}. \qquad (3)$$

Известен следующий способ непосредственного вычисления матриц A_n типа (3) без обращения к матрицам Сильвестра – Адамара (2).

Рекуррентно определяются матрицы C_m размера $m \times 2^m$:

$$C_1 = (0\ 1),\ C_m = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ C_{m-1} & C_{m-1} \end{pmatrix}, \qquad (4)$$

где $\mathbf{0} = (00\ldots0)$, $\mathbf{1} = (11\ldots1)$ – постоянные векторы соответствующей длины.

По правилам действия в поле F_2 вычисляем матрицу Уолша – Адамара (в аддитивной записи) как произведение матриц:

$$A_n = C_n^T \bullet C_n. \qquad (5)$$

В этой формуле первый множитель произведения (5) (транспонированная матрица C_n) трактуем как набор всех возможных коэффициентов линейных комбинаций, а второй сомножитель трактуем как набор образующих, составляющих базис векторного подпространства $S \subset \mathbb{Z}_2^N$ кодовых слов. Строки матрицы A_n служат кодовыми словами длины $N = 2^n$, а соответствующие строки матрицы C_n^T являются соответствующими кодируемыми сообщениями длины n, что и приводит к $(2^n, n)$-коду. Приведенные рассуждения можно рассматривать и как доказательство теоремы 1.

Основное преимущество этого кода состоит в максимально возможном кодовом расстоянии кода $d(K) = 2^{n-1}$, что вытекает из ортогональности [11] дискретных функций Уолша.

Кодовые сообщения легко получаются из кодовых слов выделением информационных координат с номерами 1, 2, 4, …, 2^{n-1}. Точнее процедура декодирования формулируется следующим образом.

Утверждение 1. Если кодовые сообщения есть строки матрицы C_n^T вида (4), то информационными координатами являются координаты с номерами в порядке 2^{n-1}, 2^{n-2}, …, 4, 2, 1 строк матрицы A_n кодовых слов.

Доказательство. Найдем матрицу R, выделяющую из матрицы A_n информационные столбцы. Это условие в матричном виде запишется $C_n^T = A_n \bullet R$, что можно переписать в виде $C_n^T = C_n^T \bullet C_n \bullet R$. Значит, матрицу R ищем из условия $C_n \bullet R = E$ равенства единичной матрице порядка n. Столбцы стандартного базиса в матрице C_n упорядочены под номерами 2^{n-1}, 2^{n-2}, …, 4, 2, 1, поскольку порядок координат берется слева направо. Поэтому в столбцах матрицы R размера $2^n \times n$ единицы на тех же указанных позициях, а остальные элементы – нули. Согласно формуле $C_n^T = A_n \bullet R$ номера позиций в столбцах матрицы R (при умножении справа) и есть указание на порядок информационных координат.

Именно тем, что порядок координат в общепринятом описании метода кодирования матрицами Уолша – Адамара получается обратный, вызван другой подход в определении матриц C_n, в статье [8] и пособии [9].

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Кодирование информации линейными перестановками дискретного преобразования Уолша

Если вернуться к теореме 1 и формуле (5), то можно заменить упорядоченный базис в виде строк матрицы C_n на любой другой упорядоченный базис того же n-мерного пространства кодовых слов S.

Теорема 2. Произвольная невырожденная над полем F_2 матрица K порядка n формулой $K \bullet C_n$ задает упорядоченный базис n-мерного пространства кодовых слов S, а строки матрицы

$$A(K) = C_n^T \bullet K \bullet C_n \qquad (6)$$

повторяют (в другом порядке) строки матрицы A_n, то есть множество кодовых слов S.

Доказательство. Невырожденность матрицы K гарантирует линейную независимость строк матрицы $K \bullet C_n$. Базисность строк доказана. Упорядоченность базиса берется в обратном порядке, снизу вверх по нумерации строк.

Строки матрицы C_n^T составляют полный набор возможных линейных комбинаций в виде всех 2^n возможных кодовых сообщений длины n. Произведение $C_n^T \bullet K$ дает тот же набор линейных комбинаций (за счет невырожденности K), но в другом порядке.

Замечание. Если в матрице $A(K)$ произвести перекодировку $0 \to 1$, $1 \to -1$ из аддитивного представления в мультипликативное, то получим [9] матрицу линейной перестановки ДПУ.

Таким образом, предлагается использовать аддитивное представление матрицы линейной перестановки ДПУ для шифрования информации. Отображение $C_n^T \to C_n^T \bullet K$ задает перестановку строк $A_n \to A(K)$. Обратное отображение $C_n^T \leftarrow C_n^T \bullet K$ задает обратную перестановку строк $A_n \leftarrow A(K)$, которая применяется при декодировании. При этом процедура поиска и исправления ошибок остается прежней, что позволяет использовать все существующие аппаратные средства. Секретным ключом служат кодовая матрица K и тесно связанная с ней матрица $A(K)$.

Если в одном направлении этим методом передается ключ, то для передачи информации в обратном направлении процедура шифрования может пройти по составленной программе без участия оператора. Знание ключа позволяет легко организовать декодирование.

Теорема 3. Если кодовые сообщения есть строки матрицы C_n^T вида (4), то упорядоченными информационными координатами описанного метода кодирования кодовыми словами *A(K)* вида (5) будут упорядоченные двоичные числа в столбцах матрицы K^{-1}.

Доказательство по схеме рассуждений в утверждении 1. Найдем матрицу *T*, выделяющую из матрицы *A*(*K*) информационные столбцы. Это условие в матричном виде запишется $C_n^T = A(K) \bullet T$, что перепишем в виде $C_n^T = C_n^T \bullet \bullet K \bullet C_n \bullet T$. Значит, матрицу *T* ищем из условия $K \bullet C_n \bullet T = E$. Домножив слева на обратную K^{-1} к кодовой матрице *K*, получим, что $C_n \bullet T = K^{-1}$. Значит матрица *T* при умножении справа выделяет из столбцов матрицы C_n столбцы матрицы K^{-1}. Поскольку столбцы матрицы C_n упорядочены по возрастанию чисел в двоичной системе счисления, представленных в ее столбцах, то единицы в матрице *T* на тех позициях, которые в двоичной системе счисления записаны в столбцах матрицы K^{-1}. Согласно формуле $C_n^T = A(K) \bullet T$, номера позиций в столбцах и есть указание на порядок информационных координат.

Пример. Действие теоремы 3 и принцип кодирования продемонстрируем примером для нумерации Уолша уровня 3 с кодовой матрицей $K = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. Матрица C_3 имеет вид:

$$C_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

По формуле (6) получается следующая матрица:

$$A(K) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Поскольку обратная к кодовой есть матрица $K^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, то информационные столбцы идут в порядке 1, 3, 7 (нумерация с нуля), что также легко заметить из вида матрицы *A(K)*.

Предположим, что при кодировании этим методом по каналу удаленной связи получили сообщение 001111000101101111111100 из 24 знаков. Разобьем сообщение на блоки (восьмерки бит) и получим набор кодовых сообщений: 00111100, 01011011, 11111100.

Для каждого сообщения вычисляем синдром, равный расстоянию Хэмминга этого сообщения до всех кодовых слов. Для первого сообщения 00111100 синдром будет равен: 4,4,0,4,4,4,4,4. Данный набор означает, что сообщение не содержит ошибок и совпадает с кодовым словом 00111100 под номером 2. Синдром второго сообщения 01011011 равен 5,3,5,3,5,3,1,3. Минимальное расстояние равно 1 до кодового сообщения с номером 6. Значит, в сообщении одна ошибка, исправив которую, получим 01011010. Синдром третьего сообщения 11111100 равен 6,6,2,6,4,4,4,4. Минимальное расстояние равно 2 до кодового сообщения с номером 2. Значит, в сообщении две ошибки, исправив которые, получим 00111100. После исправления ошибок и разделения на кодовые слова получим переданное сообщение 00111100, 01011010, 00111100.

Выделением координат с номерами 1, 3 и 7 получим кодируемое сообщение: 010, 110, 010.

Поскольку сообщение передавалось по открытому каналу связи, то перехватить его и исправить до 00111100, 01011010, 00111100 стандартным методом может любой пользователь. А вот выделить кодируемое сообщение – 010, 110, 010 – способен лишь обладатель ключа в виде матрицы *K* или K^{-1}.

На практике данный метод кодирования, естественно применять для уровня большего чем 3. Тогда сложность декодирования определяется числом возможных кодовых матриц.

В источнике [9] приведена следующая формула для числа различных невырожденных бинарных матриц порядка *m*:

$sb(m) = (2^m - 1)(2^m - 2)(2^m - 4). . .(2^m - 2^{m-1})$.

В частности: $sb(2) = 6$, $sb(3) = 168$, $sb(4) = 20\,160$, $sb(5) = 9\,999\,360$. В источнике [12] тот же результат (до уровня 4) вычислен компьютерным перебором. Экспоненциальный рост числа возможных кодовых матриц, а также отсутствие приемов декодирования перехваченного сообщения превращают этот метод в сложную математическую задачу.

Закрытым ключом данного метода кодирования служит кодовая матрица K. Также к секретной информации относятся тесно взаимосвязанные с ней матрицы K^{-1} и $A(K)$. Покажем метод восстановления кодовой матрицы K по матрице $A(K)$.

Сначала введем новое понятие инверсии квадратной матрицы, где принята нумерация с нуля. При операции инверсии все элементы матрицы порядка N симметрично отражаются относительно центра матрицы:

$$\alpha_{kj} \to \alpha_{N-k-1N-j-1}.$$

Другой вариант определения операции инверсии: это сначала инверсия всех строк, а потом инверсия всех столбцов.

Например, инверсия матрицы $K\begin{pmatrix}0 & 1 & 1\\ 1 & 1 & 0\\ 1 & 0 & 0\end{pmatrix}$ будет $Inv(K) = \begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 0\end{pmatrix}$.

Теорема 4. Главная подматрица матрицы $A(K)$, выделенная выборкой $(1, 2, \ldots, 2^{n-1})$, есть инверсия ее кодовой матрицы.

Доказательство. В строках матрицы C_n^T с номерами $1, 2, \ldots, 2^{n-1}$ записаны векторы стандартного базиса в обратном порядке. Например, для $n = 3$ это векторы $(0, 0, 1)$, $(0, 1, 0)$ и $(1, 0, 0)$. При умножении матрицей C_n^T на матрицу $K \bullet C_n$ слева, j-я строка произведения есть линейная комбинация строк матрицы $K \bullet C_n$ с коэффициентами, указанными в j-й строке матрицы C_n^T (метод описан в источнике [13]). Поэтому на месте строки с номером 1 матрицы $A(K)$ будет последняя строка матрицы $K \bullet C_n$, на месте строки с номером 2 – предпоследняя строка матрицы $K \bullet C_n$, на месте строки с номером 4 – третья снизу строка матрицы $K \bullet C_n$ и т. д.

Теперь аналогично рассмотрим произведение матриц $K \bullet C_n$ как умножение справа C_n на матрицу K. При правом умножении m-й столбец матрицы $K \bullet C_n$ есть линейная комбинация столбцов матрицы K с коэффициентами, указанными в m-м столбце матрицы C_n. Столбцы, выделенные той же выборкой, также будут элементами стандартного базиса. Но ввиду порядка следования этих столбцов в матрице C_n, при изменении значения m по элементам выборки $(1, 2, \ldots, 2^{n-1})$ будут получаться столбцы матрицы K в порядке $n - 1, n - 2, \ldots, 1,0$ (обратный порядок их степеней).

Доказанная теорема объясняет, почему общепринятый в теории кодирования метод определения матриц C_n, использованный в данной статье, хуже, чем новый метод определения аналогичных (но других) матриц, обозначенных тем же символом C_n [8, 9].

Если бы в качестве матриц C_n брали матрицы, определенные в источниках [8, 9], то теорема 4 формулировалась бы проще: указанная выборка выделяет кодовую матрицу (а не ее инверсию).

При применении рассмотренного метода кодирования, то есть при распространении метода с двух известных нумераций на примерно 10 миллионов (при уровне 5) нумераций ДПУ, естественно применять более удобную конструкцию определения C_n [8, 9].

ЗАКЛЮЧЕНИЕ

Итак, зная кодовое слово в качестве закрытого ключа, отправитель может построить аддитивную матрицу дискретного преобразования Уолша $A(K)$, с помощью которой закодировать сообщение и передать получателю. При декодировании любой получатель посредством существующей стандартной аппаратуры обнаруживает и исправляет ошибки передачи информации. Для уровня 5 кодовой матрицы гарантируется исправление семи ошибок в передаваемом сообщении из 32 символов. Получатель, знающий закрытый ключ K, выделяет из полученного и исправленного сообщения исходное сообщение. В случае перехвата без знания закрытого ключа существует около 10 миллионов различных вариантов

дискретных преобразований Уолша для минимальной для практики размерности кодовой матрицы порядка 5. В реальных каналах связи используется значительно больший порядок *m* кодовых матриц, что делает нереализуемым процесс дешифровки сигнала.

Список источников

1. Питерсон У. У., Уэлдон Э. Коды, исправляющие ошибки / пер. с англ. ; под ред. Р. Л. Добрушина, С. И. Самойленко. М. : Мир, 1976. 594 с.
2. Дворников С. В., Устинов А. А., Дворников С. С. и др. Анализ эффективности блоковых кодов // Вопросы радиоэлектроники. Серия: Техника телевидения. 2011. № 1. С. 63–73.
3. Леонтьев В. К., Мовсиян Г. Л., Маргарян Ж. Г. Верхняя и нижняя границы мощности кода, исправляющего ошибки алгебраического канала // ՀՀ ԳԱԱ Զեկույցներ : доклады НАН РА. 2020. Т. 120, № 1. С. 7–14.
4. Tinnirello C. Cyclic Codes: Low-Weight Codewords and Locators. PhD thesis, University of Trento, 2016. 133 p.
5. Костюков А. С., Башкиров А. В., Никитин Л. Н. и др. Помехоустойчивое кодирование в современных форматах связи // Вестник Воронежского государственного технического университета. 2019. Т. 15, № 2. С. 132–138.
6. Ceria M., Mora T., Sala M. Groebner bases and error correcting codes: from Cooper Philosophy to Degrobnerization // International Conference on Polynomial Computer Algebra. Saint Petersburg, October, 2020. P. 45–48.
7. Рацеев С. М., Иванцов А. М., Булдаковский П. А. Об алгоритмах декодирования циклических кодов // Ученые записки УлГУ. Серия Математика и информационные технологии. 2021. № 1. С. 87–101.
8. Беспалов М. С. Собственные подпространства дискретного преобразования Уолша // Проблемы передачи информации. 2010. Т. 46, № 3. С. 60–79.
9. Беспалов М. С., Скляренко В. А. Дискретные функции Уолша и их приложения. Владимир : ВлГУ, 2014. 67 с.
10. Беллман Р. Введение в теорию матриц / пер. с англ. В. Я. Катковника, Р. А. Полуэкова, М. С. Эпельмана ; под ред. В. Б. Лидвского. М. : Наука, 1969. 368 с.
11. Ахмед Н., Рао К. Р. Ортогональные преобразования при обработке цифровых сигналов. М. : Связь, 1980. 248 с.
12. Зяблицева Л. В., Корабельщикова С. Ю., Чесноков А. И. Линейные коды, исправляющие ошибки, и алгоритмы их подсчета // Эвристические алгоритмы и распределенные вычисления. 2014. Т. 1, № 3. С. 47–59.
13. Малоземов В. Н. Линейная алгебра без определителей. Квадратичная функция. СПб. : СПбГУ, 1997. 80 с.

References

1. Piterson U. U., Ueldon E. Kody, ispravlyayushchie oshibki. Trans., eds. R. L. Dobrushin, S. I. Samoylenko. Moscow: Mir, 1976. 594 p. (In Russ.).
2. Dvornikov S. V., Ustinov A. A., Dvornikov S. S. et al. Analiz effektivnosti blokovykh kodov. *Voprosy radioelektroniki. Seriya: Tekhnika televideniya*. 2011;(1):63–73. (In Russ.).
3. Leontiev V. K., Movsissian G. L., Margaryan Zh. G. Upper and lower bounds of the power of the error correction code of an algebraic channel. ՀՀ ԳԱԱ Զեկույցներ : *reports of the National academy of sciences of Armenia*. 2020;120(1):7–14. (In Russ.).
4. Tinnirello C. Cyclic Codes: Low-Weight Codewords and Locators. PhD thesis, University of Trento, 2016. 133 p.
5. Kostyukov A. S., Bashkirov A. V., Nikitin L. N. et al. Anti-interference coding in modern communication formats. *Bulletin of Voronezh State Technical University*. 2019;15(2):132–138. (In Russ.).
6. Ceria M., Mora T., Sala M. Groebner bases and error correcting codes: from Cooper Philosophy to Degrobnerization. In*: International Conference on Polynomial Computer Algebra*. Saint Petersburg, October. 2020. P. 45–48.
7. Ratseev S. M., Ivantsov A. M., Buldakovskiy P. A. Ob algoritmakh dekodirovaniya tsiklicheskikh kodov. *Uchenye zapiski UlGU. Seriya Matematika i informatsionnye tekhnologii*. 2021;(1):87–101. (In Russ.).
8. Bespalov M. S. Sobstvennye podprostranstva diskretnogo preobrazovaniya Uolsha. *Problems of Information Transmission*. 2010;46(3):60–79. (In Russ.).
9. Bespalov M. S., Sklyarenko V. A. Diskretnye funktsii Uolsha i ikh prilozheniya. Vladimir: VlGU, 2014. 67 p. (In Russ.).
10. Bellman R. Vvedenie v teoriyu matrits. Trans. V. Ya. Katkovnik, R. A. Poluekov, M. S. Epelman; Ed. V. B. Lidvskiy. Moscow: Nauka, 1969. 368 p. (In Russ.).
11. Akhmed N., Rao K. R. Ortogonalnye preobrazovaniya pri obrabotke tsifrovykh signalov. Moscow: Svyaz, 1980. 248 p. (In Russ.).
12. Zyablitseva L. V., Korabelshchikova S. Y., Chesnokov A. I. Linear error-correcting codes and algorithms for their calculations. *Evristicheskie algoritmy i raspredelennye vychisleniya*. 2014;1(3):47–59. (In Russ.).
13. Malozemov V. N. Lineynaya algebra bez opredeliteley. Kvadratichnaya funktsiya. Saint Petersburg: SPbGU, 1997. 80 p. (In Russ.).

Информация об авторах

М. С. Беспалов – доктор физико-математических наук, профессор.

К. А. Фролов – аспирант.

About the authors

M. S. Bespalov – Doctor of Sciences (Physics and Mathematics), Professor.

K. A. Frolov – Postgraduate.