Math-Net.Ru

Общероссийский математический портал

С. А. Степанов, Нелинейные коды, построенные по модифицированным матрицам Батсона–Адамара, *Дискрет. матем.*, 2006, том 18, выпуск 4, 137–147

DOI: <https://doi.org/10.4213/dm78>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.84.234.179

26 апреля 2023 г., 12:55:45

Нелинейные коды, построенные по модифицированным матрицам Батсона–Адамара

© 2006 г. С. А. Степанов

В работе построены два семейства нелинейных p -арных кодов, где p , $p \geq 3$, — простое число, получаемых из соответствующих классов модифицированных матриц Батсона–Адамара. Эти коды имеют минимальные расстояния, близкие к границе Плоткина, а также простые процедуры построения и декодирования. Для некоторых из этих кодов граница Плоткина достигается.

1. Введение

Многие преобразователи дискретных сигналов такие, как преобразования Уолша–Адамара и дискретное преобразование Фурье, основаны на использовании матриц с элементами, являющимися комплексными корнями из единицы. Эти матрицы входят в класс матриц Батсона–Адамара [2], имеющих вид

$$H = (\omega^{(i-1)(j-1)})_{1 \leq i, j \leq q},$$

где q , $q \geq 2$, — положительное целое число и ω — комплексный корень q -й степени из единицы. Класс матриц Батсона–Адамара допускает обобщение до класса коциклических обобщенных матриц Адамара с элементами в конечной абелевой группе G с операцией композиции в качестве умножения (см. [3, 5, 6]). Последний класс включает класс коциклических матриц Адамара. Фактически, матрица Батсона–Адамара H представляет собой коциклическую симметричную матрицу с элементами из циклической группы $\langle \omega \rangle$ порядка q . Различные авторы (см. [1, 4, 7]) использовали коциклические обобщенные матрицы Адамара для построения соответствующих коциклических кодов.

Пусть q , $q \geq 2$, — целое число и $\Gamma_q = \langle \omega \rangle$ — циклическая группа, порожденная примитивным корнем степени q из единицы. В [8] введено понятие модифицированных матриц Батсона–Адамара и построены два класса нелинейных кватернарных кодов с параметрами $(2^m, 2^{2m}, 2^{m-1})$ и $(2^m, 2^{2m+2}, 2^{m-1})$, которые получаются из соответствующих классов модифицированных комплексных матриц Адамара с элементами из циклической группы $\Gamma_4 = \{1, -1, i, -i\}$. В [9] автор строит два класса шестиричных кодов с параметрами $(3^m, 5^m, 2 \cdot 3^{m-1})$ и $(3^m, 6 \cdot 5^m, 2 \cdot 3^{m-1})$, соответственно, которые получаются из класса модифицированных матриц Батсона–Адамара с элементами из циклической группы Γ_6 . Аналогично, в [10] автор строит два класса пятиричных кодов с параметрами

$(3^m, 5^m, 2 \cdot 3^{m-1})$ и $(3^m, 5^{m+1}, 2 \cdot 3^{m-1})$. Минимальное расстояние для этих кодов близко к границе Плоткина.

Пусть $q, q = p \geq 3$, — простое и r — положительное целое число. В этой статье для каждого $r, 2 \leq r \leq p$, мы вводим два новых класса $\{H_{m,r}\}, \{\tilde{H}_{m,r}\}$ модифицированных матриц Батсона–Адамара $H_{m,r}, \tilde{H}_{m,r}$ с элементами из $\mathbb{F}_p$ и строим два класса $\{C_{m,r}^*\}, \{\tilde{C}_{m,r}^*\}$ нелинейных p -арных кодов $C_{m,r}^*, \tilde{C}_{m,r}^*$, которые строятся из $H_{m,r}$ и $\tilde{H}_{m,r}$, соответственно. Цель этой статьи — доказать следующее утверждение.

Теорема 1. Коды $C_{m,r}^*$ и $\tilde{C}_{m,r}^*$ имеют параметры

$$(r^m, p^m, (r-1)r^{m-1}), \quad (r^m, p^{m+1}, (r-1)r^{m-1}).$$

и исправляют любые

$$t \leq [(r-1)r^{m-1} - 1]/2$$

ошибок.

В заключение заметим, что как конструкции, так и параметры приведенных выше классов нелинейных q -арных кодов существенно зависят от разложения числа q на простые множители. В частности, если $q = p$ есть простое число, то коды $C_m = C_{m,r}$ и $\tilde{C}_m = \tilde{C}_{m,r}$ имеют наилучшие параметры по сравнению с другими кодами такого вида. С другой стороны, если q имеет достаточно много простых делителей, то построение достаточно длинных кодов приведенной выше формы по-видимому является очень сложной задачей.

2. Модифицированные матрицы Батсона–Адамара

Пусть $p, p \geq 3$, — простое число, $\omega = e^{2\pi i/p}$ — примитивный комплексный корень p -й степени из единицы и $\mathbb{Q}(\omega)$ — цикломатическое поле, полученное из поля рациональных чисел $\mathbb{Q}$ присоединением ω . Минимальным полиномом от ω над $\mathbb{Q}$ является полином

$$f(x) = 1 + x + x^2 + \dots + x^{p-1},$$

и поле $\mathbb{Q}(\omega)$ есть конечное расширение поля $\mathbb{Q}$ степени $p-1$. Множество

$$\{1, \omega, \omega^2, \dots, \omega^{p-2}\}$$

образует базис поля $\mathbb{Q}(\omega)$ над $\mathbb{Q}$, так что $\alpha \in \mathbb{Q}(\omega)$ может быть единственным образом записано в виде линейной комбинации

$$\alpha = a_0 + a_1\omega + a_2\omega^2 + \dots + a_{p-2}\omega^{p-2}$$

элементов базиса с коэффициентами $a_0, a_1, \dots, a_{p-2} \in \mathbb{Q}$.

Пусть $\mathbb{Z}$ — кольцо рациональных целых чисел. В этой статье мы работаем в кольце $\mathbb{Z}[\omega]$ алгебраических целых чисел поля $\mathbb{Q}(\omega)$. Каждый элемент $\alpha \in \mathbb{Z}[\omega]$ единственным образом представим в виде

$$\alpha = a_0 + a_1\omega + a_2\omega^2 + \dots + a_{p-2}\omega^{p-2},$$

где $a_0, a_1, \dots, a_{p-2} \in \mathbb{Z}$. Кольцо $\mathbb{Z}[\omega]$ содержит мультипликативную циклическую группу

$$C = \langle \omega \rangle = \{1, \omega, \omega^2, \dots, \omega^{p-1}\}$$

порядка p , элементы которой удовлетворяют соотношению

$$1 + \omega + \omega^2 + \dots + \omega^{p-1} = 0. \quad (1)$$

Пусть r , $2 \leq r \leq p$, — целое число. Рассмотрим матрицу Батсона–Адамара

$$H = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{p-2} & \omega^{p-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{(p-2)2} & \omega^{(p-1)2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \omega^{p-2} & \omega^{2(p-2)} & \dots & \omega^{(p-2)(p-2)} & \omega^{(p-1)(p-2)} \\ 1 & \omega^{p-1} & \omega^{2(p-1)} & \dots & \omega^{(p-2)(p-1)} & \omega^{(p-1)(p-1)} \end{pmatrix}$$

и ее $p \times r$ подматрицу

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{r-2} & \omega^{r-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{(r-2)2} & \omega^{(r-1)2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \omega^{p-2} & \omega^{2(p-2)} & \dots & \omega^{(r-2)(p-2)} & \omega^{(r-1)(p-2)} \\ 1 & \omega^{p-1} & \omega^{2(p-1)} & \dots & \omega^{(r-2)(p-1)} & \omega^{(r-1)(p-1)} \end{pmatrix}.$$

Пусть $A \otimes B$ обозначает кронекеровское произведение двух матриц A и B . Определим модифицированные матрицы Батсона–Адамара H_m и $\tilde{H}_m$ при $m = 2, 3, \dots$ рекурсивно с помощью соотношений

$$H_m = H_1 \otimes H_{m-1}$$

и

$$\tilde{H}_m = \begin{pmatrix} H_m \\ \omega H_m \\ \omega^2 H_m \\ \dots \\ \omega^{p-1} H_m \end{pmatrix},$$

где

$$H_1 \otimes H_{m-1} = \begin{pmatrix} H_{m-1} & H_{m-1} & H_{m-1} & \dots & H_{m-1} \\ H_{m-1} & \omega H_{m-1} & \omega^2 H_{m-1} & \dots & \omega^{r-1} H_{m-1} \\ H_{m-1} & \omega^2 H_{m-1} & \omega^4 H_{m-1} & \dots & \omega^{(r-1)2} H_{m-1} \\ \dots & \dots & \dots & \dots & \dots \\ H_{m-1} & \omega^{p-2} H_{m-1} & \omega^{2(p-2)} H_{m-1} & \dots & \omega^{(r-1)(p-2)} H_{m-1} \\ H_{m-1} & \omega^{p-1} H_{m-1} & \omega^{2(p-1)} H_{m-1} & \dots & \omega^{(r-1)(p-1)} H_{m-1} \end{pmatrix}.$$

Ясно, что H_m и $\tilde{H}_m$ — $p^m \times r^m$ и $p^{m+1} \times r^m$ матрицы с элементами из циклической группы $C = \{1, \omega, \omega^2, \dots, \omega^{p-1}\}$. Пусть

$$H_1^* = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \dots & \omega^{-(p-2)} & \omega \\ 1 & \omega^{-2} & \omega^{-4} & \dots & \omega^{-2(p-2)} & \omega^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & \omega^{-(r-2)} & \omega^{-(r-2)2} & \dots & \omega^{-(r-2)(p-2)} & \omega^{r-2} \\ 1 & \omega^{-(r-1)} & \omega^{-(r-1)2} & \dots & \omega^{-(r-1)(p-2)} & \omega^{r-1} \end{pmatrix}$$

— преобразование Эрмита матрицы H_1 , где $\omega^{-\mu}$ — элемент ω^v группы C такой, что $0 \leq v \leq p-1$ и $\mu + v \equiv 0 \pmod{p}$.

Рассмотрим теперь самосопряженную $p \times p$ матрицу

$$J_1 = H_1 H_1^* = (\gamma_{kl})_{1 \leq k, l \leq p},$$

где

$$\gamma_{kl} = \sum_{s=0}^{r-1} \omega^{(k-1)s} \omega^{-(l-1)s} = \sum_{s=0}^{r-1} e^{2\pi i(k-l)s/p},$$

и заметим, что $\gamma_{k,k} = r$, $k = 1, 2, \dots, p$, и

$$\Re \gamma_{kl} = \sum_{s=0}^{r-1} \cos \frac{2\pi(k-l)s}{p} \leq 1 + (r-1) \cos \frac{2\pi}{p}, \quad k \neq l.$$

Наконец, определим комплексные самосопряженные матрицы J_m при $m = 2, 3, \dots$ рекурсивно с помощью соотношения

$$J_m = J_1 \otimes J_{m-1}.$$

Поскольку $H_1 \otimes H_1^* = J_1$, мы видим, что

$$H_m H_m^* = J_m \tag{2}$$

для любого $m \geq 1$.

Последнее соотношение показывает, что матрицы H_m и $\tilde{H}_m$ не принадлежат классу обобщенных матриц Адамара. С другой стороны, легко показать, используя индукцию по m , что справедливо следующее утверждение.

Предложение 1. Для любого $m \geq 1$ справедливо равенство

$$J_m^* = J_m.$$

Элементы матриц J_m являются целыми алгебраическими числами $\gamma_{kl} \in \mathbb{Z}[\omega]$ вида

$$\gamma_{kl} = c_{kl}^{(0)} + c_{kl}^{(1)}\omega + \dots + c_{kl}^{(p-2)}\omega^{p-2},$$

где $c_{kl}^{(0)}, c_{kl}^{(1)}, \dots, c_{kl}^{(p-2)} \in \mathbb{Z}$ и все диагональные элементы $\gamma_{k,k}$ матрицы J_m равны r^m . Действительные части элементов γ_{kl} , не лежащих на диагонали не превосходят $(1 + (r-1) \cos(2\pi/p))r^{m-1}$.

Этот результат и соотношение (2) показывают, что матрицы H_m имеют ряд свойств, которые во многом аналогичны основным свойствам классических матриц Адамара.

3. Модифицированные коды Адамара

Пусть H_m и $\tilde{H}_m$ — модифицированные матрицы Батсона–Адамара, определенные в предыдущей секции. Модифицированный p -арный код Адамара C_m^* определяется как множество всех столбцов преобразования Эрмита H_m^* матрицы H_m . Аналогично, модифицированный p -арный код $\tilde{C}_m^*$ состоит из всех столбцов преобразования Эрмита $\tilde{H}_m^*$ матрицы

$\tilde{H}_m$. Ясно, что C_m^* , $\tilde{C}_m^*$ — нелинейные (r^m, p^m, d) и (r^m, p^{m+1}, d) коды. Найдем минимальное расстояние Хемминга d кодов C_m^* и $\tilde{C}_m^*$. Построим матрицу

$$H_m = \begin{pmatrix} H_{m-1} & H_{m-1} & H_{m-1} & \dots & H_{m-1} \\ H_{m-1} & \omega H_{m-1} & \omega^2 H_{m-1} & \dots & \omega^{r-1} H_{m-1} \\ H_{m-1} & \omega^2 H_{m-1} & \omega^4 H_{m-1} & \dots & \omega^{(r-1)2} H_{m-1} \\ \dots & \dots & \dots & \dots & \dots \\ H_{m-1} & \omega^{p-2} H_{m-1} & \omega^{2(p-2)} H_{m-1} & \dots & \omega^{(r-1)(p-2)} H_{m-1} \\ H_{m-1} & \omega^{p-1} H_{m-1} & \omega^{2(p-1)} H_{m-1} & \dots & \omega^{(r-1)(p-1)} H_{m-1} \end{pmatrix}$$

и рассмотрим ее как упорядоченное множество строк. Следующий результат играет центральную роль в последующих рассуждениях.

Теорема 2. Пусть α_k и α_l — две строки матрицы H_m , а ω^σ и ω^τ — два элемента группы $C = \{1, \omega, \dots, \omega^{p-1}\}$. Если $\omega^\sigma \alpha_k \neq \omega^\tau \alpha_l$, то расстояние Хемминга между $\omega^\sigma \alpha_k$ и $\omega^\tau \alpha_l$ не меньше $(r-1)r^{m-1}$.

Доказательство. Докажем теорему индукцией по m . Легко видеть, что утверждение верно при $m = 1$. Пусть теперь $m \geq 2$. Предположим, что расстояние Хемминга между различными строками матриц $\omega^\sigma H_{m-1}$ и $\omega^\tau H_{m-1}$ не меньше $(r-1)r^{m-2}$, и докажем, что минимальное расстояние Хемминга между различными строками матриц $\omega^\sigma H_m$ и $\omega^\tau H_m$ не меньше $(r-1)r^{m-1}$.

Рассмотрим подматрицы

$$H_{m-1}^{(0,0,\dots,0)} = (H_{m-1} \quad H_{m-1} \quad \dots \quad H_{m-1})$$

и

$$H_{m-1}^{(0,\mu,\dots,(r-1)\mu)} = (H_{m-1} \quad \omega^\mu H_{m-1} \quad \dots \quad \omega^{(r-1)\mu} H_{m-1}), \quad 1 \leq \mu \leq p-1,$$

матрицы H_m . Если a_k — элемент of H_{m-1} и ω^μ — элемент C , то, как следует из вышесказанного, произвольная строка a_k матрицы H_m может быть лишь строкой одного из видов

$$\alpha_k = (a_k \quad a_k \quad \dots \quad a_k), \quad \alpha_k = (a_k \quad \omega^\mu a_k \quad \dots \quad \omega^{(r-1)\mu} a_k), \quad 1 \leq \mu \leq p-1. \quad (3)$$

Предположим, что расстояние Хемминга между различными векторами $\omega^\sigma a_k$ и $\omega^\tau a_l$, где $a_k, a_l \in H_{m-1}$, $\omega^\sigma, \omega^\tau \in C$, не меньше $(r-1)r^{m-2}$ и докажем, что тогда расстояние Хемминга между различными векторами $\omega^\sigma \alpha_k$ и $\omega^\tau \alpha_l$, где $\alpha_k, \alpha_l \in H_m$, не меньше $(r-1)r^{m-1}$. Рассмотрим

$$\begin{aligned} \alpha_k &= (a_k \quad \omega^\mu a_k \quad \dots \quad \omega^{(r-1)\mu} a_k), \\ \alpha_l &= (a_l \quad \omega^\nu a_l \quad \dots \quad \omega^{(r-1)\nu} a_l), \\ \omega^\sigma \alpha_k &= (\omega^\sigma a_k \quad \omega^{\sigma+\mu} a_k \quad \dots \quad \omega^{\sigma+(r-1)\mu} a_k), \\ \omega^\tau \alpha_l &= (\omega^\tau a_l \quad \omega^{\tau+\nu} a_l \quad \dots \quad \omega^{\tau+(r-1)\nu} a_l) \end{aligned}$$

и заметим, что расстояние Хемминга между $\omega^\sigma \alpha_k$ и $\omega^\tau \alpha_l$ равно

$$\begin{aligned} d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) &= d(\omega^\sigma a_k, \omega^\tau a_l) \\ &\quad + d(\omega^{\sigma+\mu} a_k, \omega^{\tau+\nu} a_l) + \dots + d(\omega^{\sigma+(r-1)\mu} a_k, \omega^{\tau+(r-1)\nu} a_l). \end{aligned}$$

Заметим также, что если $\omega^\sigma a_k = \omega^\tau a_l$, то $\sigma = \tau$ и $a_k = a_l$. Действительно, так как первые компоненты векторов a_k и a_l равны 1, из этого равенства следует, что $\sigma = \tau$, откуда $a_k = a_l$. Для того чтобы найти нетривиальную нижнюю границу для $d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l)$, где $\omega^\sigma \alpha_k \neq \omega^\tau \alpha_l$, рассмотрим следующие четыре случая.

Случай 1. Пусть $(\mu, \nu) = (0, 0)$. Тогда

$$d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) = rd(\omega^\sigma a_k, \omega^\tau a_l),$$

так что из неравенства $d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) \neq 0$ следует, что $d(\omega^\sigma a_k, \omega^\tau a_l) \neq 0$. Если $l = k$ и $\sigma \neq \tau$, то $d(\omega^\sigma a_k, \omega^\tau a_k) = r^{m-1}$ и поэтому

$$d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) = r^m > (r-1)r^{m-1}.$$

Если $l \neq k$, то по предположению индукции

$$d(\omega^\sigma a_k, \omega^\tau a_l) \geq (r-1)r^{m-2},$$

откуда следует, что

$$d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) \geq (r-1)r^{m-1}.$$

Случай 2. Пусть $\mu = 0$ и ν — ненулевой элемент множества $\{0, 1, 2, \dots, p-1\}$. Рассмотрим следующие подслучаи.

(а) Пусть $\omega^\sigma a_k \neq \omega^{\tau+\rho\nu} a_l$ для всех $\rho = 0, 1, 2, \dots, r-1$. По предположению индукции

$$d(\omega^\sigma a_k, \omega^{\tau+\rho\nu} a_l) \geq (r-1)r^{m-2}, \quad 1 \leq \rho \leq r-1,$$

и поэтому

$$d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) \geq (r-1)r^{m-1}.$$

(б) Пусть $\omega^\sigma a_k = \omega^\tau a_l$. Тогда $\sigma = \tau$, $a_k = a_l$, откуда следует, что

$$\begin{aligned} d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) &= d(\omega^\sigma a_k, \omega^{\sigma+\nu} a_k) + \dots + d(\omega^\sigma a_k, \omega^{\sigma+(r-1)\nu} a_k) \\ &= (r-1)r^{m-1}. \end{aligned}$$

Аналогично, если $\omega^\sigma a_k = \omega^{\tau+\delta\nu} a_l$ для некоторого $\delta \in \{1, 2, \dots, r-1\}$, то

$$d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) = \sum_{\rho=0, \rho \neq \delta}^{r-1} d(\omega^{\tau+\delta\nu} a_l, \omega^{\tau+\rho\nu} a_l) = (r-1)r^{m-1}.$$

(в) Если $\omega^\sigma a_k = \omega^{\tau+\delta\nu} a_l, \dots, \omega^\sigma a_k = \omega^{\tau+\lambda\nu} a_l$, где $0 \leq \delta < \dots < \lambda \leq r-1$, то опять $\omega^{\delta\nu} a_l = \omega^{\lambda\nu} a_l$, что невозможно.

Случай 3. Пусть $\nu = 0$ и μ — ненулевой элемент множества $\{0, 1, \dots, p-1\}$. Эта ситуация симметрична одной из ситуаций случая 2, поэтому опять справедливо неравенство

$$d(\omega^\sigma \alpha_k, \omega^\tau \alpha_l) \geq (r-1)r^{m-1}.$$

Случай 4. Пусть $\mu \neq \nu$ — ненулевые элементы множества $\{0, 1, \dots, p-1\}$. Рассмотрим следующие подслучаи.

(а) Пусть $\omega^{\sigma+\rho\mu}a_k \neq \omega^{\tau+\rho\nu}a_l$ для всех $\rho = 0, 1, 2, \dots, r-1$. По предположению индукции

$$d(\omega^{\sigma+\rho\mu}a_k, \omega^{\tau+\rho\nu}a_l) \geq (r-1)r^{m-2}, \quad 0 \leq \rho \leq r-1,$$

откуда следует, что

$$d(\omega^\sigma a_k, \omega^\tau a_l) \geq (r-1)r^{m-1}.$$

(б) Пусть $\omega^\sigma a_k = \omega^\tau a_l$. Тогда $\sigma = \tau$, $a_k = a_l$, и поэтому

$$\begin{aligned} d(\omega^\sigma a_k, \omega^\tau a_l) &= d(\omega^{\sigma+\mu}a_k, \omega^{\sigma+\nu}a_k) + \dots + d(\omega^{\sigma+(r-1)\mu}a_k, \omega^{\sigma+(r-1)\nu}a_k) \\ &= (r-1)r^{m-1}. \end{aligned}$$

Аналогично, если $\omega^{\sigma+\delta\mu}a_k = \omega^{\tau+\delta\nu}a_l$ для некоторого $\delta \in \{1, 2, \dots, r-1\}$, то

$$\omega^{\sigma+\rho\mu}a_k = \omega^{\tau+(\rho-\delta)\mu+\delta\nu}a_l,$$

откуда следует, что

$$d(\omega^\sigma a_k, \omega^\tau a_l) = \sum_{\rho=0, \rho \neq \delta} d(\omega^{\tau+(v-\mu)\delta+\rho\mu}a_l, \omega^{\tau+\rho\nu}a_l) = (r-1)r^{m-1}.$$

(в) Если $\omega^{\sigma+\delta\mu}a_k = \omega^{\tau+\delta\nu}a_l, \dots, \omega^{\sigma+\lambda\mu}a_k = \omega^{\tau+\lambda\nu}a_l$ для $0 \leq \delta < \dots < \lambda \leq r-1$, то опять $\omega^{\delta(v-\mu)} = \omega^{\lambda(v-\mu)}$, что невозможно.

Доказательство теоремы завершено.

Следствие 1. Коды C_m^* и $\tilde{C}_m^*$ имеют, соответственно, параметры

$$(r^m, p^m, (r-1)r^{m-1}), \quad (r^m, p^{m+1}, (r-1)r^{m-1}).$$

Доказательство. Достаточно только найти минимальное расстояние d кодов C_m^* и $\tilde{C}_m^*$. Ясно, что минимальное расстояние Хемминга кода C_m^* равно минимальному расстоянию кода $\tilde{C}_m^*$ и равно минимальному расстоянию Хемминга между строками матрицы H_m . Теперь результат следует из теоремы 2.

Наряду с C_m^* и $\tilde{C}_m^*$ можно также рассматривать нелинейные коды C_m и $\tilde{C}_m$, состоящие соответственно из строк модифицированных матриц Батсона–Адамара H_m и $\tilde{H}_m$. Коды C_m , $\tilde{C}_m$ имеют те же параметры, что и C_m^* , $\tilde{C}_m^*$, а также аналогичные процедуры декодирования.

Теорема 3. Коды C_m и $\tilde{C}_m$ имеют, соответственно, параметры

$$(r^m, p^m, (r-1)r^{m-1}), \quad (r^m, p^{m+1}, (r-1)r^{m-1})$$

и исправляют любые

$$t \leq [(r-1)r^m - 1]/2$$

ошибок.

Ясно, что если $a_k = (a_{k,1}, \dots, a_{k,r^m})$ — вектор кода C_m и $\bar{a}_l^\tau = (\bar{a}_{l,1}, \dots, \bar{a}_{l,r^m})^\tau$ — вектор кода C_m^* , то

$$a_k \bar{a}_l = \sum_{j=1}^{r^m} a_{kj} \bar{a}_{lj} = \gamma_{kl},$$

где γ_{kl} — соответствующий элемент матрицы J_m .

4. Алгоритм декодирования

Коды C_m^* , $\tilde{C}_m^*$ и C_m , $\tilde{C}_m$ допускают очень эффективную процедуру декодирования. Декодерирующие алгоритмы для C_m^* , $\tilde{C}_m^*$ и C_m , $\tilde{C}_m$ совершенно аналогичны, поэтому мы ограничимся описанием декодирующего алгоритма для C_m^* .

Пусть

$$H_m = (a_{kl}), \quad 1 \leq k \leq p^m, \quad 1 \leq l \leq r^m,$$

— определенные выше $p^m \times r^m$ матрицы Батсона–Адамара с элементами из $C = \langle \omega \rangle$, где ω — примитивный корень p -й степени из 1. Пусть

$$\bar{a}_{k_0}^\tau = (\bar{a}_{k_0,1}, \dots, \bar{a}_{k_0,r^m})^\tau \in C_m^*$$

— переданный кодовый вектор и

$$\bar{c}^\tau = (\bar{c}_1, \dots, \bar{c}_{r^m})^\tau$$

— принятый вектор, отличающийся от $\bar{a}_k^\tau$ в t позициях. Как обычно, мы предполагаем, что канал с шумом преобразует каждый символ $\bar{a}_{kl}$ алфавита

$$C = \{1, \omega, \dots, \omega^{p-1}\}$$

в другой символ алфавита C с одной и той же малой вероятностью p^* и не изменяет $\bar{a}_{kl}$ с вероятностью $1 - p^*$.

Чтобы восстановить переданный вектор $\bar{a}_{k_0}^\tau$ по принятому вектору $\bar{c}^\tau$, мы вычитаем $\bar{c}^\tau$ из каждого столбца $\bar{a}_k^\tau$ матрицы H_m^* и рассматриваем полученную матрицу

$$S_m^* = (\bar{a}_{kl} - \bar{c}_k)^\tau, \quad 1 \leq k \leq p^m, \quad 1 \leq l \leq r^m.$$

Так как элементы матрицы H_m^* и компоненты вектора $\bar{c}^\tau$ являются элементами циклической группы $C = \langle \omega \rangle$, $S_m^* = (\bar{s}_{kl})^\tau$ есть $r^m \times p^m$ комплексная матрица с элементами

$$\bar{s}_{kl} = s_{kl}^{(0)} + s_{kl}^{(1)}\omega + \dots + s_{kl}^{(p-2)}\omega^{p-2}$$

из кольца $\mathbf{Z}[\omega]$.

Рассмотрим множество столбцов

$$\bar{s}_k^\tau = (\bar{s}_{k,1}, \bar{s}_{k,2}, \dots, \bar{s}_{k,r^m})^\tau = (\bar{a}_{k,1} - \bar{c}_1, \bar{a}_{k,2} - \bar{c}_2, \dots, \bar{a}_{k,r^m} - \bar{c}_{r^m})^\tau$$

матрицы S_m^* . Если число искаженных компонент принятого вектора $\bar{c}^\tau$ равно

$$t \leq [(d-1)/2] = [(r-1)r^{m-1} - 1]/2],$$

то расстояние Хемминга $d(\bar{a}_{k_0}, \bar{c})$ между векторами $\bar{a}_{k_0} = (\bar{a}_{k_0,1}, \bar{a}_{k_0,2}, \dots, \bar{a}_{k_0,r^m})$ и $\bar{c} = (\bar{c}_1, \bar{c}_2, \dots, \bar{c}_{r^m})$ равно t . Отсюда следует, что столбец

$$\bar{s}_{k_0}^\tau = \bar{a}_{k_0}^\tau - \bar{c}^\tau = (\bar{s}_{k_0,1}, \bar{s}_{k_0,2}, \dots, \bar{s}_{k_0,r^m})^\tau$$

матрицы S_m^* имеет ровно t ненулевых компонент. С другой стороны, если $k \neq k_0$, то

$$(r-1)r^{m-1} \leq d(\bar{a}_k, \bar{a}_{k_0}) \leq d(\bar{a}_k, \bar{c}) + d(\bar{c}, \bar{a}_{k_0}) = d(\bar{a}_k, \bar{c}) + t,$$

откуда следует, что

$$d(\bar{a}_k, \bar{c}) \geq (r-1)r^{m-1} - t > t.$$

Следовательно, любой столбец $\bar{a}_k$ матрицы S_m^* с $k \neq k_0$ содержит по меньшей мере $t+1$ ненулевых компонент. Это свойство матрицы S_m^* приводит к следующему простому алгоритму декодирования.

- (1) Для того чтобы восстановить переданный вектор $\bar{a}_{k_0}$, рассматриваем множество столбцов матрицы S_m^* и выбираем единственный столбец

$$\bar{s}_{k_0} = (\bar{s}_{k_0,1}, \bar{s}_{k_0,2}, \dots, \bar{s}_{k_0,r^m})^T$$

с минимальным числом t ненулевых компонент.

- (2) Затем декодируем полученный вектор $\bar{c}^T$, полагая его равным столбцу

$$\bar{a}_{k_0}^T = (\bar{a}_{k_0,1}, \bar{a}_{k_0,2}, \dots, \bar{a}_{k_0,r^m})^T$$

матрицы H_m^* , соответствующему выбранному столбцу матрицы S_m^* .

Ясно, что код C_m^* исправляет любые

$$t \leq [(d-1)/2] = [(r-1)r^{m-1} - 1]/2]$$

ошибок. Аналогично, код $\tilde{C}_m^*$ с параметрами $(r^m, p^{m+1}, (r-1)r^{m-1})$ также исправляет

$$t \leq [(r-1)r^{m-1} - 1]/2]$$

ошибок. В этом случае матрица

$$S_m^* = (\bar{s}_{kl})^T = (\bar{a}_{kl} - \bar{c}_l)^T$$

представляет собой $r^m \times p^{m+1}$ комплексную матрицу с элементами из кольца $\mathbf{Z}[\omega]$.

В заключение заметим, что в действительности описанный выше алгоритм использует только операцию вычитания алгебраических целых чисел кольца $\mathbf{Z}[\omega]$ и не требует умножения или деления. По этой причине алгоритм декодирования является достаточно быстрым.

5. Пример

В этом разделе приводится простой пример, иллюстрирующий приведенный выше алгоритм декодирования. Пусть

$$r = 3, \quad p = 5, \quad C = \{1, \omega, \omega^2, \omega^3, \omega^4\},$$

и

$$H_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & \omega \\ 1 & \omega^4 & \omega^3 \end{pmatrix}.$$

Рассмотрим матрицу

$$H_2 = \begin{pmatrix} H_1 & H_1 & H_1 \\ H_1 & \omega H_1 & \omega^2 H_1 \\ H_1 & \omega^2 H_1 & \omega^4 H_1 \\ H_1 & \omega^3 H_1 & \omega H_1 \\ H_1 & \omega^4 H_1 & \omega^3 H_1 \end{pmatrix}$$

и перепишем ее в виде

$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & \omega & 1 & \omega^3 & \omega & 1 & \omega^3 & \omega \\ 1 & \omega^4 & \omega^3 & 1 & \omega^4 & \omega^3 & 1 & \omega^4 & \omega^3 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \omega^4 & \omega^4 & \omega^4 & \omega^3 & \omega^3 & \omega^3 \\ 1 & \omega & \omega^2 & \omega^4 & 1 & \omega & \omega^3 & \omega^4 & 1 \\ 1 & \omega^2 & \omega^4 & \omega^4 & \omega & \omega^3 & \omega^3 & 1 & \omega^2 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 & 1 & \omega^3 & \omega & \omega^4 \\ 1 & \omega^4 & \omega^3 & \omega^4 & \omega^3 & \omega^2 & \omega^3 & \omega^2 & \omega \end{pmatrix}.$$

Код C_2^* состоит из столбцов $3^2 \times 5^2$ матрицы H_2^* и имеет параметры $(3^2, 5^2, 2 \cdot 3)$. Покажем, что код C_2^* исправляет одну или две ошибки. Рассмотрим вектор $\bar{a}^\tau \in C_2^*$, скажем,

$$\bar{a}_3^\tau = (1, \omega^3, \omega, 1, \omega^3, \omega, 1, \omega^3, \omega)^\tau$$

и предположим, что этот вектор передается по каналу с шумом. Пусть

$$\bar{c}^\tau = (1, \omega^3, \omega, 1, \omega^3, \omega, 1, \omega, \omega^4)^\tau$$

— полученный вектор, отличающийся от переданного вектора $\bar{a}^\tau$ в двух последних позициях. Для исправления ошибок, вычтем $\bar{c}^\tau$ из каждого столбца $\bar{a}_k^\tau$ матрицы H_2^* . В результате получим матрицу

$$S_2^* = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 1 - \omega^3 & \omega^4 - \omega^3 & 0 & \omega^2 - \omega^3 & \dots & \omega^2 - \omega^3 & \omega - \omega^3 \\ 1 - \omega & \omega^3 - \omega & 0 & \omega^4 - \omega & \dots & \omega^4 - \omega & \omega^2 - \omega \\ 0 & 0 & 0 & 0 & \dots & \omega - 1 & \omega - 1 \\ 1 - \omega^3 & \omega^4 - \omega^3 & 0 & \omega^2 - \omega^3 & \dots & 0 & \omega^2 - \omega^3 \\ 1 - \omega & \omega^3 - \omega & 0 & \omega^4 - \omega & \dots & 1 - \omega & \omega^3 - \omega \\ 0 & 0 & 0 & 0 & \dots & \omega^2 - 1 & \omega^2 - 1 \\ 1 - \omega & \omega^4 - \omega & \omega^3 - \omega & \omega^2 - \omega & \dots & \omega^4 - \omega & \omega^3 - \omega \\ 1 - \omega^4 & \omega^3 - \omega^4 & \omega - \omega^4 & 0 & \dots & \omega - \omega^4 & 0 \end{pmatrix}$$

с элементами, принадлежащими $\mathbf{Z}[\omega]$. Третий столбец этой матрицы имеет только две ненулевые компоненты и любой другой столбец матрицы S_2^* содержит не меньше трех ненулевых компонент. Согласно алгоритму декодирования мы декодируем полученный вектор $\bar{c}^\tau$ и полагаем его равным третьему столбцу

$$\bar{a}_3^\tau = (1, \omega^3, \omega, 1, \omega^3, \omega, 1, \omega^3, \omega).$$

матрицы H_2^* .

Список литературы

1. Baliga A., New self-dual codes from cocyclic Hadamard matrices. *J. Comb. Math. Comb. Comput.* (1982) **28**, 7–14.
2. Butson K. T., Generalized Hadamard matrices. *Proc. Amer. Math. Soc.* (1962) **13**, 894–898.
3. Elliot K. F., Rao R. R., *Fast transforms: algorithms, analyses, applications*. Academic Press, New York, 1982.
4. Horadam K. J., Udaya P., Cocyclic Hadamard codes. *IEEE Trans. Inform. Theory* (2000) **46**, 1545–1550.
5. De Launcy W., Generalized Hadamard matrices whose rows and columns form a group. *Lecture Notes Math.* (1983) **1036**, 154–176.
6. Maslen D. K., Rockmore D. N., Generalized FFTs—a survey of some recent results. *DIMACS* (1997) **28**, 183–237.
7. Pinnawala N., Rao A., Cocyclic simplex codes of type α over $\mathbb{Z}_4$ and $\mathbb{Z}_2$. *IEEE Trans. Inform. Theory* (2004) **50**, 2165–2169.
8. Stepanov S. A., A new class of quaternary codes. *Inform. Transm. Probl.* (2006) **42**, №1, 3–12.
9. Stepanov S. A., A new class of nonlinear senary codes. *Inform. Transm. Probl.* (2006) **42**, №2, 53–62.
10. Степанов С. А., Новый класс пятеричных кодов. *Дискретная математика* (2005) **17**, №4, 7–17.

Статья поступила 22.06.2005.

Переработанный вариант поступил 13.06.2006.