Информационные процессы, Том 12, № 1, 2012, стр. 98–104.

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Сигнально-кодовая конструкция для системы множественного доступа, использующей векторный канал с аддитивным белым гауссовским шумом

В.В. Зяблов, А.А. Фролов

Институт проблем передачи информации, Российская академия наук, Москва, Россия
Поступила в редколлегию 23.03.2012

Аннотация—В работе рассматривается проблема построения системы множественного доступа, использующей векторный канал с аддитивным белым гауссовским шумом. Для решения этой задачи предложена сигнально-кодовая конструкция на основе кода с малой плотностью проверок (МПП-кода) над полем GF(Q) и проведено ее исследование методом имитационного моделирования.

1. ВВЕДЕНИЕ

Рассмотрим следующую модель канала. Предполагается, что канал состоит из q независимых непересекающихся частотных подканалов. Кроме того, предполагается, что несколько пользователей могут одновременно передавать информацию по этому каналу (мы будем обозначать число пользователей через S), причем в каждый момент времени каждый из пользователей выбирает один из частотных подканалов для передачи.

Заметим, что такая модель канала допускает и более широкую трактовку. Так входы канала можно рассматривать как комплексные векторы длины q, причем каждый элемент такого вектора можно ассоциировать как с некоторой частотой, так и с временным слотом (в этом случае последовательность состояний некоторого слота во времени можно рассматривать как подканал во временной области, по аналогии с подканалом в частотной области).

Пусть в некоторый момент времени на входе канала S векторов $\mathbf{x}_i = (x_{(i,1)}, x_{(i,2)}, \ldots, x_{(i,q)}) \in \mathbb{C}^q, i = 1, \ldots, S$, тогда на выходе мы имеем вектор $\mathbf{y} = (y_1, y_2, \ldots, y_q) \in \mathbb{C}^q$, причем

$$y_j = \sum_{i=1}^{S} x_{(i,j)} + N_j, j = 1, \ldots, q,$$

где $N_j = N(0, \sigma^2)$ – двумерный ($N_j \in \mathbb{C}$) аддитивный белый гауссовский шум (АБГШ) с математическим ожиданием 0 и дисперсией σ^2.

Целями настоящей работы являются создание сигнально-кодовой конструкции, использующей канал вышеописанного типа, и исследование свойств системы множественного доступа, построенной на основе такой конструкции, методом имитационного моделирования.

2. ОПИСАНИЕ СИГНАЛЬНО-КОДОВОЙ КОНСТРУКЦИИ

Будем рассматривать описанную выше модель векторного канала, в которой S пользователей синхронно передают векторы. Ниже мы будем предполагать, что все пользователи используют один и тот же конечный алфавит – символы поля $GF(Q)$, где $Q = q^k, k \in \mathbb{N}$ (значение параметра k будет уточнено позднее).

Передача. Обозначим через C_O внешний МПП-код [1, 2] с параметрами $[N, K = RN]$ над полем $GF(Q)$, через C_I внутренний код с параметрами $[n, k = rn]$ над полем $GF(q)$, причем $Q = q^k$. Кодирование полученного в результате каскадного кода $C_O \diamondsuit C_I$ производится в два этапа: сначала кодируем K информационных символов с помощью кода C_O, затем каждый из N символов полученного слова C_I (один символ внешнего кода соответствует k символам внутреннего, так как $Q = q^k$). Заметим, что полученный код имеет длину nN и скорость rR.

После кодирования мы имеем слово длины nN над полем $GF(q)$. Каждому символу поставим в соответствие комплексный вектор длины q, в котором ровно одно значение в позиции, соответствующей данному символу поля $GF(q)$ (мы предполагаем, что элементы вектора занумерованы элементами поля и этот порядок фиксирован и одинаков для всех пользователей; обозначим отображение, ставящее в соответствие элементу поля элемент вектора через ξ), отлично от нуля. В качестве этого значения выберем комплексное число с единичной амплитудой и случайной фазой. Перед передачей каждого вектора в канал выполняется случайная перестановка. Перестановки, используемые каждым из пользователей, выбираются равновероятно и независимо из всего множества возможных перестановок (при передаче каждого символа используется своя перестановка); используемые конкретным пользователем перестановки неизвестны никому кроме пары "приемник-передатчик".

Интервал времени за которое передается один вектор (а следовательно и поставленный ему в соответствие q-ичный символ) будем называть тактом. Мы будем предполагать, что в системе используется тактовая синхронизация.

Прием. Базовая станция последовательно принимает сообщения от всех пользователей. Рассмотрим процесс приема сообщения, пришедшего от i-го пользователя. Будем полагать, что принимающая станция засинхронизирована с передатчиком каждого из пользователей. Это означает, что приемнику известны nN столбцов, которые соответствуют кодовому слову, переданному i-м пользователем. При приеме каждого столбца выполняется перестановка, обратная той, что использовал i-ый пользователь при передаче. Таким образом, получим матрицу $\mathbf{Y}$ размера $q \times nN$. Процесс декодирования разбивается на два этапа:

Декодирование внутреннего кода. Последовательно декодируем N внутренних кодов C_I. Покажем это на примере одного их них (пусть без ограничения общкости это будет первый код). Пусть матрица $\mathbf{Y}_1$ размера $q \times n$ состоит из первых n столбцов матрицы $\mathbf{Y}$. Далее от матрицы $\mathbf{Y}_1$ перейдем к матрице $\mathbf{Y}'$, $y'(i,j) = |y_1(i,j)|, \forall i = 1, \ldots, q; j = 1, \ldots, n$ (иными словами $\mathbf{Y}'$ – это матрица модулей). Теперь для каждого $c_I^{(t)} \in C_I, t = 1, \ldots, q^k$ вычислим значение L_t следующим образом

$$L_t = \sum_{j=1}^{n} y' \left(\xi \left(\mathbf{c}_I^{(t)}(j) \right), j \right).$$

Выберем слово с максимальным L_t. Процесс подсчета L_t для слова $c_I^{(t)} = (1, 0, 2, 1, 3)$ показан на Рис. 1.

Декодирование внешнего кода. Для декодирования внешнего МПП-кода на полем $GF(Q)$ используем алгоритм распространения доверия $(\mathscr{A}_{BP})$[1] над полем $GF(Q)$. Этот алгоритм исследовался в работах [3–6]. Подробное описание алгоритма приведено в приложении. Для того, чтобы применить этот алгоритм необходимо знать канал, а точнее переходные вероятности. В данном случае канал для внешнего кода мы не знаем, поэтому сделаем два существенных упрощения:

– После декодирования внутренних кодов примем жесткое решение по каждому из символов внешнего кода. Заметим, что если код C_I является равновесным, то мы получим Q-ичный

[1] В англоязычной литературе исрользуется термин "belief propagation".

$$\mathbf{Y}' = \begin{array}{|c|c|c|c|c|}\hline y'(1,1) & y'(1,2) & y'(1,3) & y'(1,4) & y'(1,5) \\ \hline y'(2,1) & y'(2,2) & y'(2,3) & y'(2,4) & y'(2,5) \\ \hline y'(3,1) & y'(3,2) & y'(3,3) & y'(3,4) & y'(3,5) \\ \hline y'(4,1) & y'(4,2) & y'(4,3) & y'(4,4) & y'(4,5) \\ \hline \end{array}$$

Рис. 1. Процесс подсчета L_t для слова $c_I^{(t)} = (1, 0, 2, 1, 3)$

симметричный канал (QСК), в котором МПП-коды на полем $GF(Q)$ существенно лучше МПП, построенных над другими полями;

– Будем использовать фиксированные переходные вероятности, которые подбираются экспериментально. К примеру мы можем проводить испытания, увеличивая E_b/N_0 и оценивая вероятности перехода, и выбрать вероятности такими, что наши требования к вероятности ошибки на блок (символ, бит) впервые выполняются. Интуитивно понятно, что для больших E_b/N_0 требования также будут выполнены.

Даже при сделанных допущениях алгоритм $\mathscr{A}_{BP}$ оказывается существенно лучше алгоритмов из [9].

Замечание 1. Заметим, что прием кодового слова от некоторого пользователя инициируется лишь в том случае, если этот пользователь действительно передавал информацию в системе.

Замечание 2. Заметим, что наличие блоковой синхронизации между пользователями, передающими информацию, не предполагается (в этом отношении предложенная нами система похожа на систему множественного доступа, описанную в [7]), поэтому, вообще говоря, принимающая станция должна быть засинхронизирована с каждым из пользователей ведущих передачу в рассматриваемой системе, т.е. фактически каждому из них должен соответствовать отдельный приемник.

Замечание 3. В реальной системе для того, чтобы перестановки были известны и на приемнике и на передатчике целесообразно использовать засинхронизированные генераторы псевдослучайных чисел, которые традиционно применяются в системах связи, основанных на псевдослучайном переключении частот [8].

В следующем разделе приведен пример такой системы, на Рис. 2 приведена блок схема предложенной системы.

3. РЕЗУЛЬТАТЫ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Зафиксируем следующие параметры: $Q = 64$; $N = 510$; $R = 0,5$; $q = 64$, $n = 8$, $r = 1/8$ (в качестве внутреннего кода используется код с повторением над $GF(64)$, который является равновесным). Переходные вероятности выбраны так, что вероятность ошибки на блок меньше

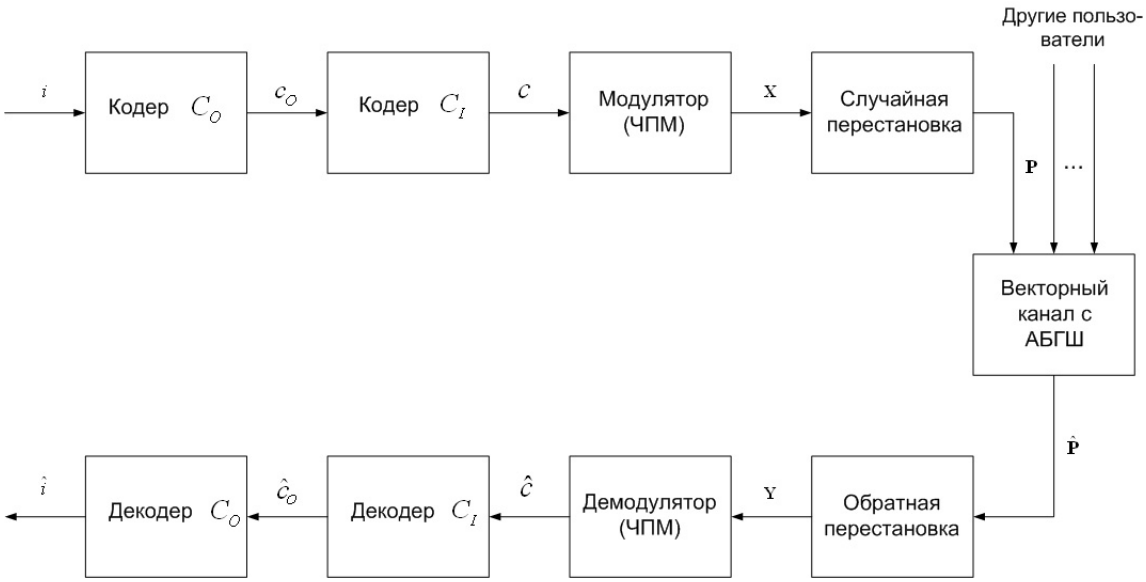

Рис. 2. Блок схема предложенной СКК

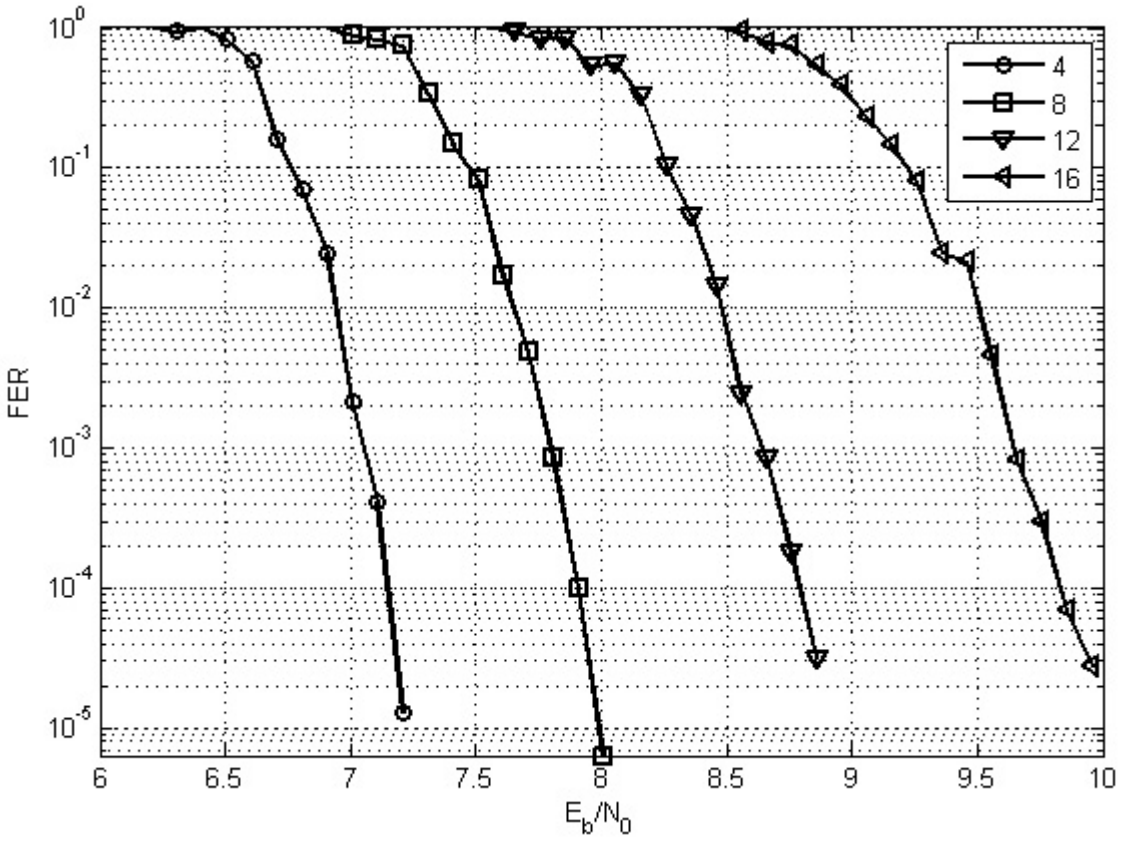

Рис. 3. Вероятность ошибки на блок от E_b/N_0

10^{-4}. На Рис. 3, Рис. 4, Рис. 5 приведены полученные результаты. На каждом из рисунков приведено по четыре зависимости при $S = 4, 8, 12, 16$.

Пусть требуется, чтобы вероятность ошибки на блок была меньше 10^{-4}, приведем значения E_b/N_0, при которых это требование выполняется

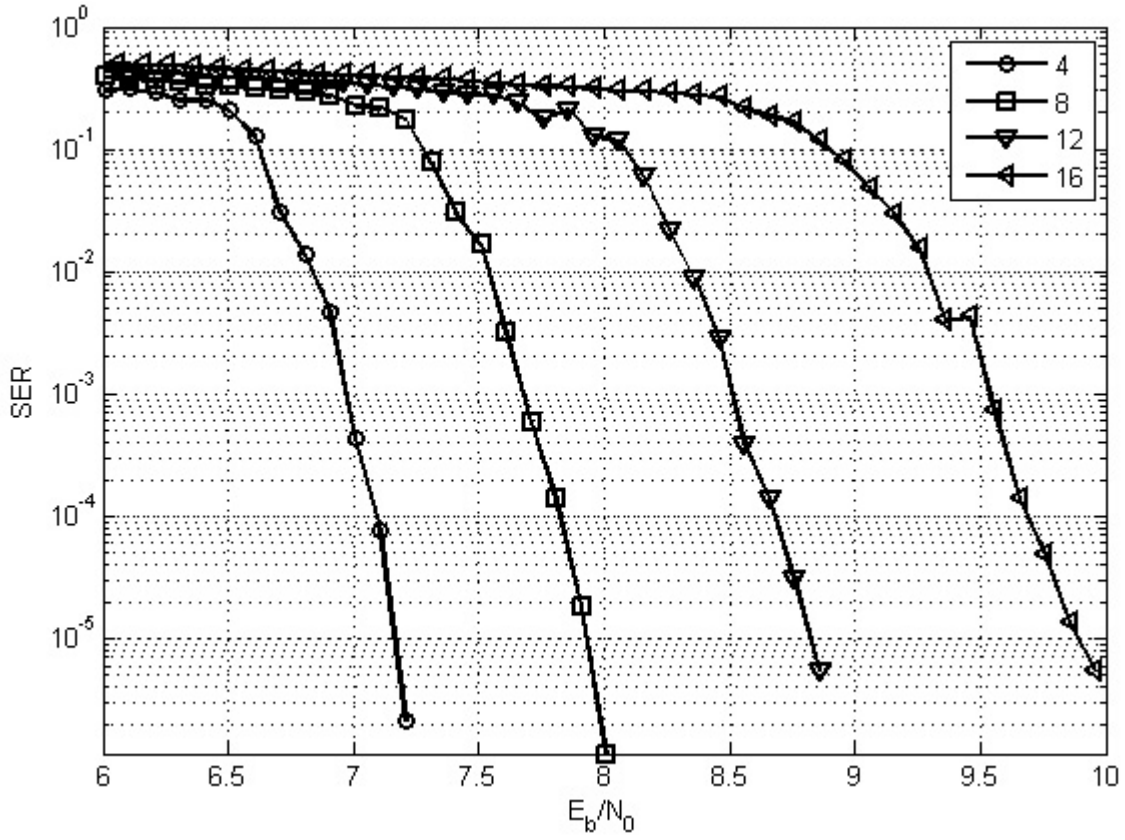

Рис. 4. Вероятность ошибки на символ от E_b/N_0

Таблица 1. Зависимость E_b/N_0 от S

S	4	8	12	16
E_b/N_0, дБ	7,16	7,91	8,81	9,86

ПРИЛОЖЕНИЕ

Здесь мы подробно опишем алгоритм $\mathscr{A}_{BP}$ декодирования МПП-кода с параметрами $[N, K]$, построенного над полем $GF(Q)$:

Входные данные: Последовательность из априорных условных распределений для каждого из символов принятого слова. Под распределением случайной величины x при условии, что принята величина y, мы понимаем вектор следующего вида

$$\mathbf{r}\,(x|y) = \left(p\,(x=0|y)\,,\, p\,(x=1|y)\,, p\,(x=\alpha|y)\,, \ldots, p\left(x=\alpha^{Q-2}|y\right)\right),$$

где y – принятое значение.

Входные данные алгоритма можно представить в виде вектора

$$\mathbf{r}^{(0)} = \left(\mathbf{r}^{(0)}\,(x_1|y_1)\,,\, \mathbf{r}^{(0)}\,(x_2|y_2)\,, \ldots, \mathbf{r}^{(0)}\,(x_N|y_N)\right),$$

где верхний индекс обозначает номер итерации (в данном случае индекс 0, говорит о том, что это входные данные).

Инициализация Введем две вспомогательные матрицы $M = \mu_{(j,k)}$ размера $\ell \times N$ и $T = \tau_{(j,k)}$ размера $n_0 \times (N-K)$, содержащих соотвеиственно сообщения от символьных вершин

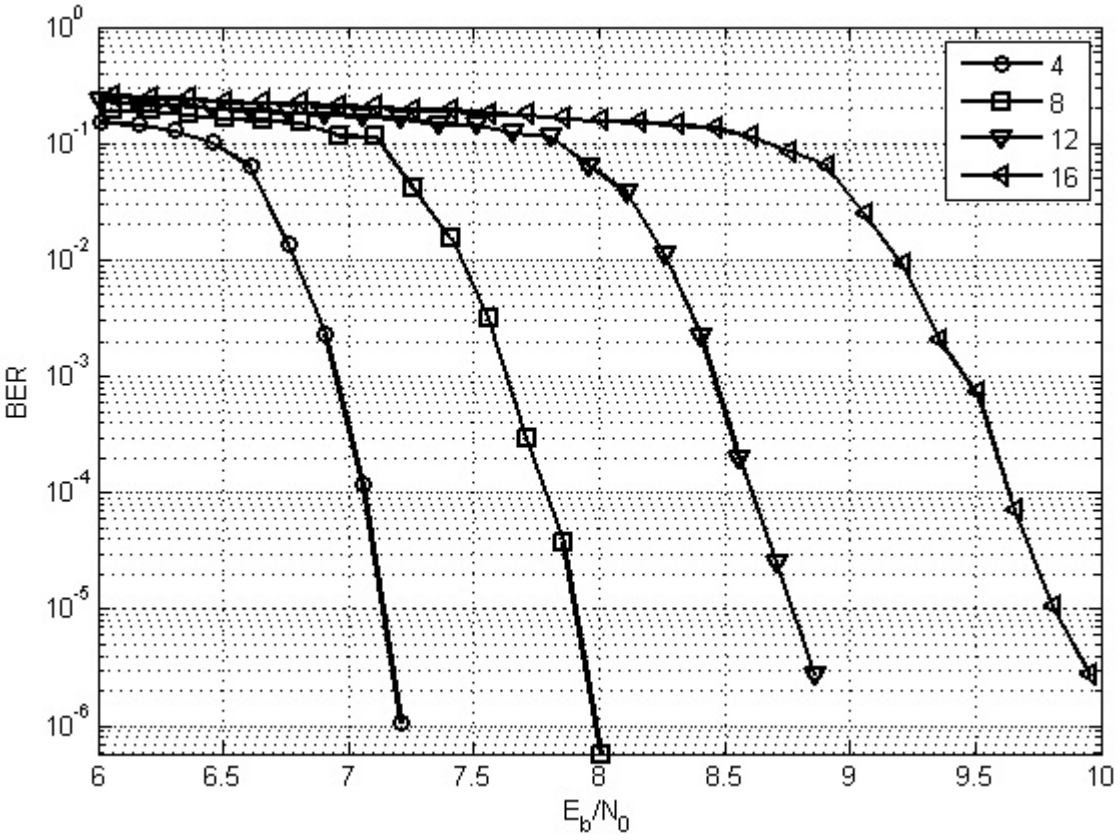

Рис. 5. Вероятность ошибки на бит от E_b/N_0

к проверочным и от проверочных к символьным. На первой итерации элементы матрицы M инициализируются так

$$\mu_{(j,k)} = \mathbf{r}^{(0)}(x_k|y_k), j = 1, ..., \ell$$

Итерация цикла: Каждая итерация разбивается на два этапа:

Обработка сообщений в проверочных вершинах: Рассмотрим обработку сообщений в первой проверочной вершине. Эта вершина имеет степень n_0, т.е. с ней соединены n_0 символьных вершин. От каждой символьной вершины j, соединенной с данной проверочной вершиной, в данную проверочную вершину приходит сообщение μ_j с информацией о распределении для символа j. Для каждого из символов, входящих в данную вершину мы вычисляем новое распределение, используя текущие. Покажем это на примере трех символьных вершин x_1, x_2 и x_3. Пусть проверочная вершина, накладывает ограничение следующего вида

$$h_1x_1 + h_2x_2 + h_3x_3 = 0,$$

где $h_i \in GF(Q), i = 1, ..., 3$. Вычислим апостериорное распределение для x_1. Для этого перепишем проверочное соотношение в виде

$$x_1 = -h_1^{-1}(h_2x_2 + h_3x_3).$$

Таким образом,

$$x_1 = -h_1^{-1}(z_2 \otimes z_3),$$

где $z_2 = h_2x_2$, $z_3 = h_3x_3$, легко видеть что распределения для z_2 и z_3 получаются с помощью перестановки элементов распределений, соответствующих ненулевым элементам поля, для x_2 и x_3. Операция $\otimes$ – это операция циклической свертки в конечном поле.

Для остальных проверочных вершин поступаем аналогично. Записываем полученные распределения в сообщения τ_i для символьных вершин.

Обработка сообщений в символьных вершинах:

Для каждой символьной вершины у нас есть ℓ сообщений τ_j с информацией о распределении для этого символа. Вычислим апостепиорное распределение для символов. Покажем на примере x_1

$$\mathbf{r}^{(i)}(x_1) = \mathbf{r}^{(0)}(x) \odot \left(\bigodot_{j=1}^{\ell} \tau_j \right),$$

где $\odot$ – операция поэлементного умножения векторов.

Сообщения для проверочных вершин

$$\mu_k = \mathbf{r}^{(0)}(x) \odot \left(\bigodot_{1 \leqslant j \leqslant \ell, j \neq k} \tau_j \right).$$

Условие выхода из цикла: После каждой итерации вычисляем синдром текущего слова (для этого необходимо принять жесткое решение для каждого из символов $\mathbf{r}^{(i)}$, т.е. выбрать символ с наибольшей вероятностью). Если синдром равен нулю, то выдать текущий вектор $\mathbf{r}^{(i)}$. Кроме того, если счетчик числа итераций больше некоторой заранее заданной величины, а синдром так и не стал нулевым – выдать отказ от декодирования.

Выходные данные: Вектор $\mathbf{r}^{(i)}$, где i – номер последней итерации.

Замечание 4. Самой сложной частью алгоритма является обработка проверочных вершин. Вычисление напрямую циклической свертки двух случайных величин в конечном поле потребует порядка $\mathcal{O}(Q^2)$ операций, однако эту операцию можно существенно ускорить ($\mathcal{O}(Q \log_2 Q)$), применив многомерное преобразование Фурье.

СПИСОК ЛИТЕРАТУРЫ

1. *Галлагер Р. Дж.* Коды с малой плотностью проверок на четность. М.: Мир, 1966.
2. *Tanner R.* A Recursive Approach to Low Complexity Codes // IEEE Trans. Inform. Theory. 1981. V. 27. № 5. P. 533 – 547.
3. *Davey M., MacKay D.J.C.* Low Density Parity Check Codes over GF(q) // IEEE Commun. Lett. 1998. V. 2. № 6. P. 165–167.
4. *Barnault L., Declercq D.* Fast Decoding Algorithm for LDPC over GF (2q) // The Proc. 2003 Inform. Theory Workshop. 2003. P. 70–73.
5. *Wymeersch H., Steendam H., Moeneclaey M.* Log-Domain Decoding of LDPC Codes over GF(q) // The Proc. IEEE Intern. Conf. on Commun. 2004. P. 772–776.
6. *Declercq D., Fossorier M.* Decoding Algorithms for Nonbinary LDPC Codes Over GF(q) // IEEE Trans. Communications. 2007. V. 55. № 4. P. 633–643.
7. *Бассалыго Л. А.* Модель ограниченного асинхронного множественного доступа при наличии ошибок // Пробл. передачи информ. 2009. Т. 45. №1. С. 41–50.
8. *Zigangirov K. Sh.* Theory of Code Division Multiple Access Communication // John Whiley and Sons, Piscataway, New Jersey, 2004.
9. *Зяблов В.В., Рыбин П.С., Фролов А.А.* Алгоритм декодирования с вводом стираний для МПП-кодов, построенных над полем GF(q) // Информационно-Управляющие Системы. 2011. Т. 50, № 1. С. 62–68.