УДК 621.391.251
doi:10.15217/issn1684-8853.2017.2.58

ОБ ОДНОЙ КОНСТРУКЦИИ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ С ЦИКЛИЧЕСКОЙ СТРУКТУРОЙ МАКРОБЛОКОВ

Д. О. Иванов[a], *инженер-программист*
А. В. Козлов[a], *ведущий инженер-программист*
А. А. Овчинников[a], *канд. техн. наук, доцент*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Постановка проблемы: *современные инфокоммуникационные системы требуют достижения высоких скоростей передачи информации с обеспечением при этом высокой надежности, т. е. низкого уровня вероятности ошибки. Для борьбы с помехами, возникающими в канале связи, традиционно используют коды, исправляющие ошибки. Одним из наиболее мощных и одновременно эффективных современных средств помехозащищенного кодирования являются коды с малой плотностью проверок на четность. Однако требование достижения крайне высоких скоростей передачи информации ставит задачу построения не просто кодов, хорошо исправляющих ошибки и имеющих простые процедуры кодирования и декодирования, а конструктивно ориентированных на возможности более эффективной реализации, в том числе аппаратной.* ***Цель исследования:*** *построение эффективных кодов с малой плотностью, структура которых позволяет оптимизировать существующие архитектуры декодеров.* ***Результаты:*** *предложена модификация конструкции кодов с малой плотностью на основе кодов Рида — Соломона, обладающая циклической структурой макроблоков. Показано, как данная структура может быть использована для оптимизации архитектуры частично параллельного декодера, основанного на многоуровневом алгоритме распространения доверия.* ***Практическая значимость:*** *предложенные конструкция и архитектура декодера позволяют достигать низких вероятностей ошибки декодирования в высокоскоростных системах передачи информации (таких, например, как оптические каналы связи).*

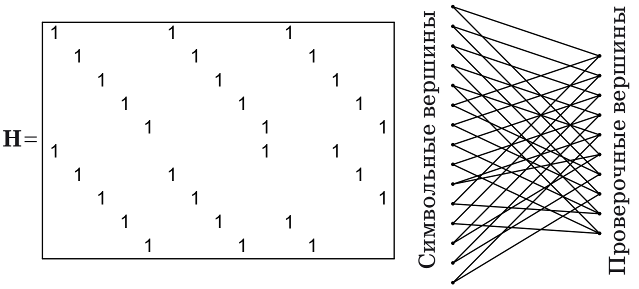
Ключевые слова *— коды с малой плотностью проверок на четность, коды с циклической структурой макроблоков, многоуровневый алгоритм распространения доверия, архитектура частично параллельных декодеров.*

Введение

Коды с малой плотностью проверок на четность (low-density parity-check codes — LDPC) были предложены Р. Галлагером в ранних 60-х годах прошлого века [1, 2], однако были забыты вплоть до конца столетия, так как эффективность этих кодов начинает существенно проявляться с увеличением их длины, сегодня достигая значений от тысяч до сотен тысяч бит, а вычислительные возможности того времени не позволяли работать с такими длинами. С ростом производительности вычислительной техники за последние 15–20 лет LDPC-коды стали одним из основных изучаемых классов помехоустойчивого кодирования, как широко распространенным в существующих стандартах связи [3–8], так и предлагаемым для использования в перспективных, таких как мобильная связь пятого поколения (5G) или оптическая проводная связь.

Проверочная матрица LDPC-кода обладает свойством разреженности, т. е. содержит малое количество ненулевых элементов. Р. Галлагер показал, что коды с таким свойством хотя и имеют, как правило, небольшое минимальное расстояние, могут достигать высоких уровней помехозащищенности, используя итеративные посимвольные алгоритмы декодирования. Такие алгоритмы могут использоваться как в жестком (двоичный симметричный канал — ДСК), так и в полунепрерывном каналах связи (канал с АБГШ — аддитивным белым гауссовым шумом), а также для исправления стираний. Один из самых распространенных алгоритмов декодирования для канала с АБГШ был предложен Р. Галлагером и называется алгоритмом распространения доверия (belief propagation — BP) [1, 2, 9].

Итеративные посимвольные декодеры для LDPC-кодов обычно описываются с помощью графа Таннера [10], являющегося двудольным графом, задаваемым проверочной матрицей кода как матрицей инцидентности (рис. 1). Граф Таннера состоит из двух множеств вершин, символьных и проверочных. Алгоритмы декодирования описываются как вычисление сообщений в узлах графа и пересылка вычисленных сообщений по ребрам графа. На вероятность ошибки таких декодеров могут влиять различные структуры графа, такие как длина минимального цикла (обхват графа) [11], распределение весов ребер [12–14], блокирующие и останавливающие множества [15, 16]. Простейшим ограничением, накладываемым на структуру кода, является отсутствие в графе Таннера циклов длиной 4, т. е. с учетом четности длин циклов двудольного графа обхват графа должен быть равен по меньшей мере 6.



■ *Рис. 1.* Проверочная матрица LDPC-кода и соответствующий ей граф Таннера

На сегодняшний день известно множество конструкций LDPC-кодов, однако, несмотря на наличие некоторых эвристических подходов к их построению, для получения эффективных кодов с заданными параметрами используют интенсивный компьютерный поиск и компьютерное моделирование.

Одним из самых общих подходов, сложившихся за последние годы, является использование проверочной матрицы, состоящей из блоков матриц перестановки (так называемых блочно-перестановочных конструкций), и дальнейшее ее маскирование нулевыми блоками для варьирования весовых распределений, цикловых структур графа и т. п. [11, 17]. Это позволяет строить, как правило, квазициклические коды, для которых возможны эффективные процедуры кодирования и декодирования.

Сегодня известно множество модификаций алгоритма распространения доверия, некоторые из которых призваны уменьшить вероятность ошибки декодирования, некоторые — упростить вычисления и реализацию [18–21]. Одной из таких модификаций является многоуровневый алгоритм распространения доверия (layered belief propagation — L-BP) [22, 23]. При построении архитектур декодеров актуальными являются так называемые частично параллельные декодеры, использующие компромисс между выигрышем от распараллеливания и количеством вычислительных элементов. В данной статье рассматриваются блочно-перестановочные конструкции LDPC-кодов, обладающие дополнительным свойством — циклической структурой макроблоков в проверочной матрице. На основе этой структуры рассматривается упрощение архитектуры частично параллельного декодера для алгоритма L-BP.

Блочно-перестановочные коды, основанные на кодах Рида — Соломона

В последние годы одним из наиболее исследуемых и применяемых подходов к построению LDPC-кодов является использование так называемой блочно-перестановочной конструкции [11, 17, 24, 25]. Основой такой конструкции является проверочная матрица кода, имеющая вид

$$\mathbf{H}=\begin{bmatrix}\mathbf{C}_{11} & \mathbf{C}_{12} & \dots & \mathbf{C}_{1\rho}\\ \mathbf{C}_{21} & \mathbf{C}_{22} & \dots & \mathbf{C}_{2\rho}\\ \dots & \dots & \dots & \dots\\ \mathbf{C}_{\gamma 1} & \mathbf{C}_{\gamma 2} & \dots & \mathbf{C}_{\gamma\rho}\end{bmatrix}, \qquad (1)$$

где $\mathbf{C}_{i,j}$ — произвольные подматрицы. Чаще всего в качестве подматриц выбираются перестановочные матрицы, если же они являются степенями матрицы циклической перестановки

$$\mathbf{C}=\begin{bmatrix}0 & 0 & 0 & \dots & 0 & 1\\ 1 & 0 & 0 & \dots & 0 & 0\\ 0 & 1 & 0 & \dots & 0 & 0\\ \dots & \dots & \dots & \dots & \dots & \dots\\ 0 & 0 & 0 & \dots & 1 & 0\end{bmatrix},$$

то коды, задаваемые (1), являются квазициклическими, что облегчает процедуры кодирования и декодирования, а также задает структуру для комбинаторного анализа таких кодов. Коды, задаваемые матрицей (1), являются регулярными LDPC-кодами с весом столбца γ и весом строки ρ, однако, заменив некоторые подматрицы в (1) на нулевые (такая процедура называется маскированием), можно получить нерегулярные коды, что позволяет улучшить качество работы итеративного декодера.

В работе [26] предложена следующая комбинаторная конструкция для построения блочно-перестановочных LDPC-кодов на основе кодов Рида — Соломона (RS-LDPC). Рассмотрим код Рида — Соломона (РС) над полем GF(q) длиной $n = q - 1$ с двумя информационными символами. Известно [27, 28], что такой код имеет минимальное расстояние $d_{\text{РС}} = n - 1$, это значит, что любые два кодовых слова либо различны во всех позициях, либо совпадают не более чем в одной позиции. В дальнейшем будем рассматривать укороченный РС-код длиной ρ, где $\rho \le n$. Будем считать, что элементы поля GF(q) заданы целыми числами $\{0, 1, 2, ..., q - 1\}$, где 0 и 1 — ноль и единица поля, а для всех остальных чисел справедливо $i = \alpha^{i-1}$, α — примитивный элемент поля.

Из укороченного (ρ, 2) РС-кода выберем кодовое слово $\mathbf{a}$ веса ρ и составим множество

$$C_1 = \{\beta\mathbf{a}\colon \beta \in \text{GF}(q),\ \beta \ne 0,1\}.$$

Множество C_1 состоит из q векторов веса ρ, любая пара векторов различается во всех позициях. Разобьем линейное векторное пространство C, состоящее из кодовых слов (ρ, 2) РС-кода, на смежные классы C_i, $i = 2, ..., q$ по пространству C_1. Для элемента $\alpha \in$ GF(q) зададим характеристический вектор $\mathbf{c}(\alpha)$ длиной q с единицей на позиции α

и нулями на всех остальных позициях. Пусть $a_{t,j}(s)$ — j-й символ ($j = 0, ..., \rho - 1$) s-го вектора ($s = 1, ..., q$) смежного класса C_t, тогда сформируем матрицу $\mathbf{H}^{(t)}$ следующим образом:

$$H^{(t)} = \begin{bmatrix} c(a_{t,0}(1)) & c(a_{t,1}(1)) & \dots & c(a_{t,\rho-1}(1)) \\ c(a_{t,0}(2)) & c(a_{t,1}(2)) & \dots & c(a_{t,\rho-1}(2)) \\ \dots & \dots & \dots & \dots \\ c(a_{t,0}(q)) & c(a_{t,1}(q)) & \dots & c(a_{t,\rho-1}(q)) \end{bmatrix}. \quad (2)$$

Зададим проверочную матрицу RS-LDPC-кода как

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}^{(1)} \\ \mathbf{H}^{(2)} \\ \dots \\ \mathbf{H}^{(\gamma)} \end{bmatrix}. \quad (3)$$

Такой код является регулярным LDPC-кодом с весом строк ρ и весом столбцов γ. По построению обхват графа Таннера для этого кода не менее 6. Из (1) и (2) матрица $\mathbf{H}$ состоит из блоков

$$\mathbf{C}_{i,j} = \begin{bmatrix} \mathbf{c}(a_{j,i}(1)) \\ \mathbf{c}(a_{j,i}(2)) \\ \dots \\ \mathbf{c}(a_{j,i}(q)) \end{bmatrix},$$

являющихся матрицами перестановки. В следующем разделе мы покажем, как на основе этой конструкции можно построить квазициклические LDPC-коды, обладающие циклической структурой макроблоков.

Макроблоковые LDPC-коды на основе RS-LDPC-кодов

Рассмотрим модификацию конструкции RS-LDPC, описанной в предыдущем разделе. Как и ранее, конструкция основана на $(n, 2)$ РС-коде над полем GF(q), $n = q - 1$. Код Рида — Соломона имеет подкод, являющийся кодом с повторением, состоящий из кодовых слов

$$\mathbf{c}_1 = (0, 0, ..., 0),$$
$$\mathbf{c}_2 = (1, 1, ..., 1),$$
$$\dots$$
$$\mathbf{c}_q = (q-1, q-1, ..., q-1).$$

Возьмем любое кодовое слово $\mathbf{a}$ кода РС, не принадлежащее коду с повторением, и сформируем матрицу

$$\mathbf{X} = \begin{bmatrix} \mathbf{a}+\mathbf{c}_1 \\ \mathbf{a}+\mathbf{c}_2 \\ \dots \\ \mathbf{a}+\mathbf{c}_q \end{bmatrix}.$$

Матрица $\mathbf{X}$ является $(q \times q - 1)$-матрицей над GF(q), ее строками являются кодовые слова РС-кода вследствие линейности этого кода. Пусть x_{ij} — элемент $\mathbf{X}$ и $\mathbf{X}_i = [x_{1i}, x_{2i}, ..., x_{qi}]^{\mathrm{T}}$ — i-й столбец $\mathbf{X}$. Зададим

$$\mathbf{Y}_i = \begin{bmatrix} \mathbf{c}(x_{1i}) \\ \mathbf{c}(x_{2i}) \\ \dots \\ \mathbf{c}(x_{qi}) \end{bmatrix},$$

где $\mathbf{c}(x_{ij})$, как и ранее, — характеристический вектор элемента $x_{ij} \in$ GF(q). Заметим, что все элементы $\mathbf{X}_i$ различны по построению, и $\mathbf{Y}_i$ — $(q \times q)$-матрица перестановки, которую мы будем называть «блоком». Более того, если q — простое число, то $\mathbf{Y}_i$ является матрицей циклической перестановки. Сформируем $(q \times q(q-1))$-матрицу

$$\mathbf{Y} = [\mathbf{Y}_1, \mathbf{Y}_2, ..., \mathbf{Y}_{q-1}],$$

полностью определяемую выбором первоначального кодового слова $\mathbf{a}$. Обозначим это кодовое слово как $\mathbf{a}^{(1)} = \mathbf{a}$, и $\mathbf{Y}^{(1)} = \mathbf{Y}$.

Выберем теперь значение γ, являющееся делителем $q - 1$. Так как РС-код является циклическим кодом, вектор $\mathbf{a}^{(2)} = \mathbf{a}^{(1)} \ggg \gamma$, являющийся циклическим сдвигом вектора $\mathbf{a}^{(1)}$ на γ позиций, также принадлежит коду РС. Повторяя для $\mathbf{a}^{(2)}$ описанные ранее шаги, получим матрицу $\mathbf{Y}^{(2)}$. Заметим, что $\mathbf{Y}^{(2)} = \mathbf{Y}^{(1)} \ggg \gamma q$. Если рассматривать матрицу $\mathbf{Y}^{(1)}$ как состоящую из блоков $\mathbf{Y}_i$, то $\mathbf{Y}^{(2)}$ — это матрица, полученная циклическим сдвигом блоков $\mathbf{Y}^{(1)}$ на γ позиций. Задавая $\mathbf{Y}^{(3)} = \mathbf{Y}^{(2)} \ggg \gamma q$ и т. д., получим матрицу

$$\mathbf{H} = \begin{bmatrix} \mathbf{Y}^{(1)} \\ \mathbf{Y}^{(2)} \\ \dots \\ \mathbf{Y}^{(\gamma)} \end{bmatrix},$$

имеющую в точности γ единиц в каждом столбце и $q - 1$ единиц в каждой строке. Взяв ρ блоков-столбцов из матрицы $\mathbf{H}$, $\rho \le q - 1$, получим (γ, ρ)-регулярный LDPC-код. Представим эту матрицу в блоковом виде, отдельно выделив $(q \times q)$-макроблоки:

$$\mathbf{H} = \left[\begin{array}{ccc|ccc|c|ccc} \mathbf{Y}_1 & \dots & \mathbf{Y}_\gamma & \mathbf{Y}_{\gamma+1} & \dots & \mathbf{Y}_{2\gamma} & \dots & \mathbf{Y}_{q-\gamma} & \dots & \mathbf{Y}_{q-1} \\ \mathbf{Y}_{q-\gamma} & \dots & \mathbf{Y}_{q-1} & \mathbf{Y}_1 & \dots & \mathbf{Y}_\gamma & \dots & \mathbf{Y}_{q-2\gamma} & \dots & \mathbf{Y}_{q-\gamma-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{Y}_{\gamma+1} & \dots & \mathbf{Y}_{2\gamma} & \mathbf{Y}_{2\gamma+1} & \dots & \mathbf{Y}_{3\gamma} & \dots & \mathbf{Y}_1 & \dots & \mathbf{Y}_\gamma \end{array}\right].$$

Перенумеровав блоки-столбцы $\mathbf{H}$ (состоящие из q столбцов каждый) от 1 до $q - 1$, переупорядочим их в соответствии со следующей перестановкой:

$$\pi = \{1, \lambda + 1, 2\lambda + 1, ..., (\gamma - 1)\lambda + 1,$$
$$2, \lambda + 2, 2\lambda + 2, ..., (\gamma - 1)\lambda + 2,$$
$$...$$
$$\lambda, 2\lambda, 3\lambda, ..., q - 1\},$$

где $\lambda = (q - 1)/\gamma$. Результат переупорядочивания даст матрицу $\mathbf{H}_{\mathrm{Macro}}$, задающую код, эквивалентный задаваемому матрицей $\mathbf{H}$ и дополнительно обладающий циклической макроблоковой структурой, которую мы проиллюстрируем на примере.

Пусть $\gamma = 3$, $\rho = 9$, $\lambda = 3$. Тогда

$$\mathbf{H} = \left[\begin{array}{ccc|ccc|ccc} \mathbf{Y}_1 & \mathbf{Y}_2 & \mathbf{Y}_3 & \mathbf{Y}_4 & \mathbf{Y}_5 & \mathbf{Y}_6 & \mathbf{Y}_7 & \mathbf{Y}_8 & \mathbf{Y}_9 \\ \mathbf{Y}_7 & \mathbf{Y}_8 & \mathbf{Y}_9 & \mathbf{Y}_1 & \mathbf{Y}_2 & \mathbf{Y}_3 & \mathbf{Y}_4 & \mathbf{Y}_5 & \mathbf{Y}_6 \\ \mathbf{Y}_4 & \mathbf{Y}_5 & \mathbf{Y}_6 & \mathbf{Y}_7 & \mathbf{Y}_8 & \mathbf{Y}_9 & \mathbf{Y}_1 & \mathbf{Y}_2 & \mathbf{Y}_3 \end{array}\right]$$

и $\pi = \{1, 4, 7, 2, 5, 8, 3, 6, 9\}$. Применяя эту перестановку, получим

$$\mathbf{H}_{\mathrm{Macro}} = \left[\begin{array}{ccc|ccc|ccc} \mathbf{Y}_1 & \mathbf{Y}_4 & \mathbf{Y}_7 & \mathbf{Y}_2 & \mathbf{Y}_5 & \mathbf{Y}_8 & \mathbf{Y}_3 & \mathbf{Y}_6 & \mathbf{Y}_9 \\ \mathbf{Y}_7 & \mathbf{Y}_1 & \mathbf{Y}_4 & \mathbf{Y}_8 & \mathbf{Y}_2 & \mathbf{Y}_5 & \mathbf{Y}_9 & \mathbf{Y}_3 & \mathbf{Y}_6 \\ \mathbf{Y}_4 & \mathbf{Y}_7 & \mathbf{Y}_1 & \mathbf{Y}_5 & \mathbf{Y}_8 & \mathbf{Y}_2 & \mathbf{Y}_6 & \mathbf{Y}_9 & \mathbf{Y}_3 \end{array}\right]. \quad (4)$$

Такая структура макроблоков может использоваться для реализации эффективных схем кодирования и декодирования.

При построении блочно-перестановочных кодов, задаваемых матрицей (1), для улучшения их свойств зачастую используется процедура маскирования, т. е. замена некоторых блоков проверочной матрицы на нулевые блоки. Это не только позволяет получить нерегулярные коды с оптимизированными весами строк и столбцов, но также может приводить к улучшению цикловой структуры соответствующего графа Таннера, так как нулевые блоки могут «разрывать» циклы небольшой длины, приводя к снижению их количества и их влияния на итеративное декодирование [17]. Помимо обычной процедуры маскирования, которая может применяться для рассмотренных конструкций, отметим следующий способ внесения нулевых блоков в проверочную матрицу $\mathbf{H}$.

Пусть $\mathbf{Y}_1 = \mathbf{Y}_2 = ... = \mathbf{Y}_\gamma = \mathbf{0}$, тогда в приведенном выше примере для $\gamma = 3$ получим

$$\mathbf{H} = \left[\begin{array}{ccc|ccc|ccc} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{Y}_4 & \mathbf{Y}_5 & \mathbf{Y}_6 & \mathbf{Y}_7 & \mathbf{Y}_8 & \mathbf{Y}_9 \\ \mathbf{Y}_7 & \mathbf{Y}_8 & \mathbf{Y}_9 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{Y}_4 & \mathbf{Y}_5 & \mathbf{Y}_6 \\ \mathbf{Y}_4 & \mathbf{Y}_5 & \mathbf{Y}_6 & \mathbf{Y}_7 & \mathbf{Y}_8 & \mathbf{Y}_9 & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array}\right].$$

После применения перестановки π получим матрицу

$$\mathbf{H}_{\mathrm{Macro}} = \left[\begin{array}{ccc|ccc|ccc} \mathbf{0} & \mathbf{Y}_4 & \mathbf{Y}_7 & \mathbf{0} & \mathbf{Y}_5 & \mathbf{Y}_8 & \mathbf{0} & \mathbf{Y}_6 & \mathbf{Y}_9 \\ \mathbf{Y}_7 & \mathbf{0} & \mathbf{Y}_4 & \mathbf{Y}_8 & \mathbf{0} & \mathbf{Y}_5 & \mathbf{Y}_9 & \mathbf{0} & \mathbf{Y}_6 \\ \mathbf{Y}_4 & \mathbf{Y}_7 & \mathbf{0} & \mathbf{Y}_5 & \mathbf{Y}_8 & \mathbf{0} & \mathbf{Y}_6 & \mathbf{Y}_9 & \mathbf{0} \end{array}\right].$$

В этой матрице нулевые блоки стоят на диагоналях макроблоков, таким образом сохраняя макроблоковую структуру кода. Данный код остается регулярным LDPC-кодом.

Архитектура декодера для кодов с циклической структурой макроблоков

Для декодирования LDPC-кодов используются итеративные посимвольные декодеры, в основе большинства которых лежит алгоритм BP [1, 2]. Однако существует множество его модификаций, нацеленных как на уменьшение вероятности ошибки декодирования, так и на упрощение его реализации. Одной из таких модификаций является алгоритм L-BP [23, 24].

Приведем описание алгоритма L-BP. Входом декодера являются логарифмы отношения правдоподобия (log-likelihood ratio — LLR) принятых символов. Пусть $\mathbf{H}$ — $(r \times n)$ проверочная матрица вида (3), состоящая из γ полос, где в каждой полосе в каждом столбце содержится не более одной ненулевой позиции. Пусть каждая полоса содержит q строк. Обозначим через $N(i)$ множество индексов ненулевых позиций в i-й строке $\mathbf{H}$, через $M(j)$ — множество индексов ненулевых позиций в j-м столбце $\mathbf{H}$. Ниже приведен алгоритм L-BP.

Вход алгоритма: LDPC-код с проверочной матрицей $\mathbf{H} = [\mathbf{H}^{(1)}, ..., \mathbf{H}^{(\gamma)}]^{\mathrm{T}}$, а также значения входных LLR λ_j для $j = 1, ..., n$.

Инициализация: в каждой символьной вершине $\Lambda_j = \lambda_j$ для $j = 1, ..., n$. В каждой проверочной вершине $R_{ij} = 0$ для всех $j \in N(i)$ и $i \in M(j)$.

Одна итерация алгоритма: каждая итерация состоит из γ подытераций, соответствующих обработке горизонтальных полос $\mathbf{H}^t$, где $t = 1, ..., \gamma$. Для каждой i-й проверки в полосе $\mathbf{H}^t$ выполнить:

Шаг 1. Для всех $j \in N(i)$ выполнить

$$Q_{ij} = \Lambda_j - R_{ij}.$$

Шаг 2. Для всех $j \in N(i)$ выполнить

$$R_{ij} = (-1)^{|N(i)|} \prod_{j' \in N(i) \setminus j} \mathrm{sign}(Q_{ij'}) \psi\left(\sum_{j' \in N(i) \setminus j} \psi(|Q_{ij'}|) \right),$$

где $\psi(x) = -\ln(\tanh(x/2))$.

Шаг 3. Для всех $j \in N(i)$ выполнить

$$\Lambda_j = Q_{ij} + R_{ij}.$$

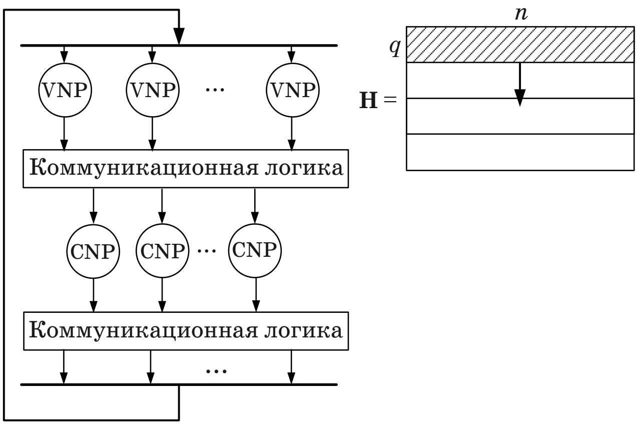
Архитектуры декодеров LDPC-кодов включают в себя модуль для обработки символьных вершин VNP (variable node processor) и модуль для обработки проверочных вершин CNP (check node processor) графа Таннера. В некоторых случаях эти модули проводят вычисления в два этапа и подразделяются на FH-VNP (first-half VNP) и SH-VNP (second-half VNP) и FH-CNP и SH-CNP соответственно.

Архитектура декодера BP (и L-BP) может реализовываться в полностью параллельном режиме, однако это требует большого количества вычислительных элементов, а также приводит к низкому коэффициенту загрузки каждого элемента. Поэтому интерес представляют так называемые частично параллельные архитектуры декодирования. Рассмотрим один из возможных подходов к организации такой архитектуры для матриц вида (3).

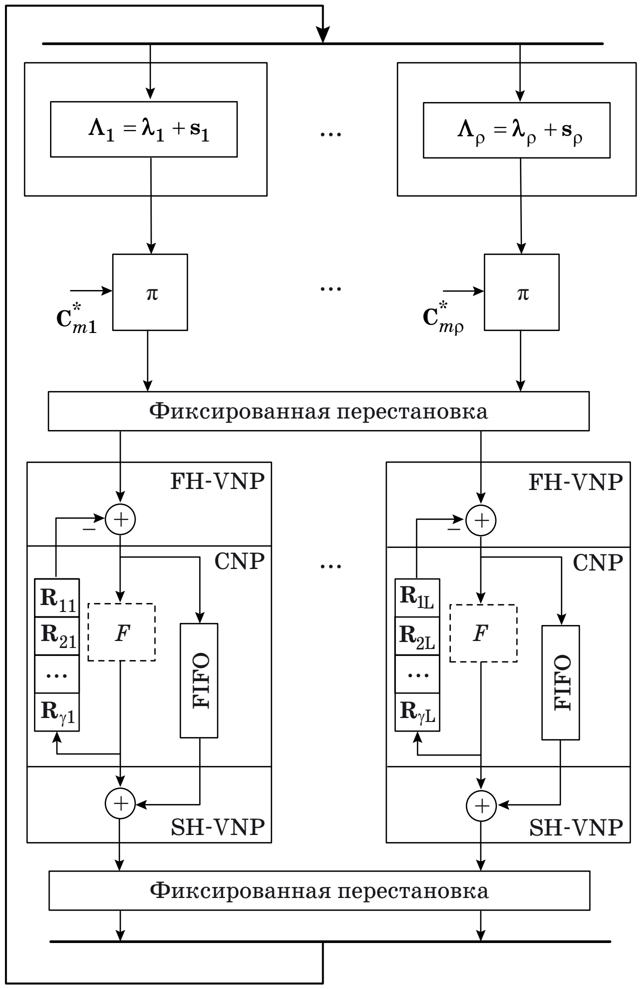
Декодер с частичной параллелизацией по проверочным вершинам обрабатывает параллельно q проверочных вершин, т. е. содержит q модулей VNP и n модулей CNP. Обработка матрицы $\mathbf{H}$ ведется последовательно от одной горизонтальной полосы к другой. Общая схема такой архитектуры приведена на рис. 2.

Для эффективного доступа к памяти вычисления нескольких символьных и проверочных вершин объединяются на одних процессорах. Чтобы учесть это, будем использовать обозначение $\boldsymbol{\lambda}_i$ вместо λ_i, а также Λ_i, $\mathbf{R}_{ij}$, $\mathbf{Q}_{ij}$ вместо соответствующих величин. Частично параллельная архитектура для L-BP-декодера приведена на рис. 3.

Перед началом работы декодера память, хранящая значения апостериорных LLR Λ_i, инициализируется подвекторами входных LLR λ_i, переставленными в соответствии с матрицами перестановки $\mathbf{C}_{\gamma i}$ последней полосы матрицы $\mathbf{H}$ (1). После окончания каждой итерации пересчитанные подвекторы LLR будут находиться в этой памяти в том же порядке, а после обработки каждой полосы (т. е. после выполнения подытерации), — в порядке, соответствующем матрицам перестановок данной полосы.



■ *Рис. 2.* Декодер с частичной параллелизацией по проверочным вершинам



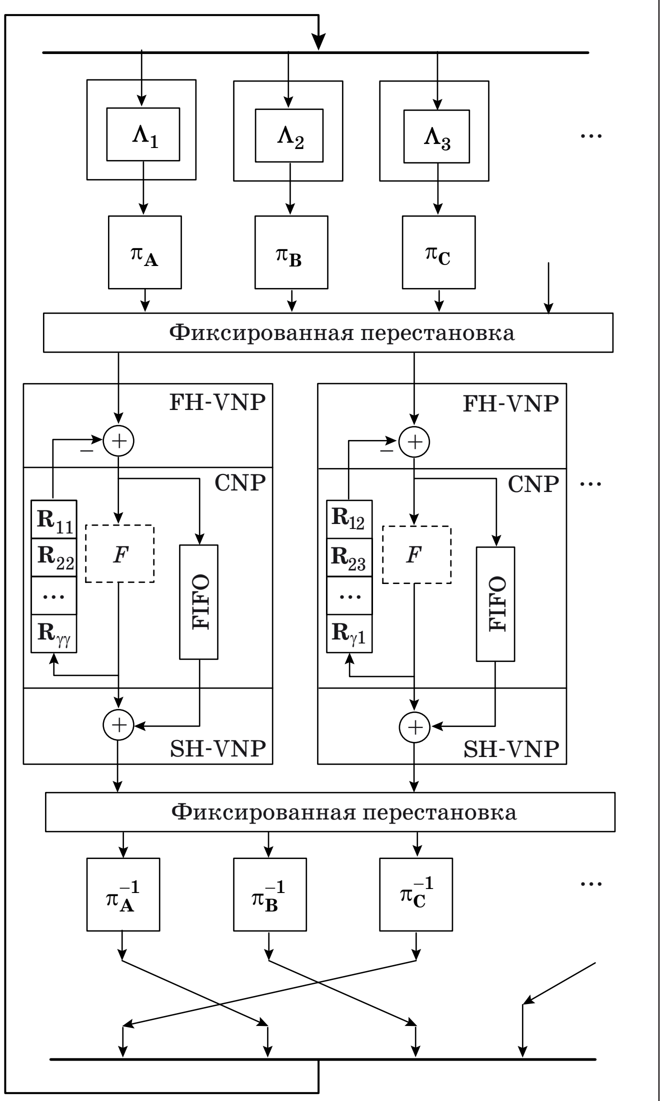
■ *Рис. 3.* Частично параллельная архитектура декодера L-BP

С учетом того, что после обработки $(m - 1)$-й полосы вектор Λ_i переставлен в памяти в соответствии с перестановкой $\mathbf{C}_{m-1,i}$, в начале обработки m-й полосы вектор Λ_i переставляется в соответствии с матрицей перестановки $\mathbf{C}^*_{mi}$ такой, что после ее применения вектор Λ_i окажется переставлен в соответствии с перестановкой $\mathbf{C}_{mi}$. Дальнейшее вычисление символьных вершин $\mathbf{Q}_{ij}$ и $\mathbf{R}_{ij}$ происходит в FH-VNP- и CNP-процессорах, при этом дополнительно сохраняются старые значения $\mathbf{Q}_{ij}$ (это необходимо, чтобы SH-VNP-процессор мог обновить значения Λ_j путем добавления к ним пересчитанных значений $\mathbf{R}_{ij}$).

Архитектура декодера L-BP может быть усовершенствована для кодов (4) с циклической структурой макроблоков. Основная цель модификации — полностью избавиться от программируемых перестановок и использовать только фиксированные, что приведет к уменьшению сложности и задержки при обработке полос проверочной матрицы.

При наличии циклической структуры макроблока проверочная матрица **H** разделена на макроблоки ($\gamma \times \gamma$), в которых каждая строка блоков является циклическим сдвигом предыдущей. Тогда архитектура декодера L-BP может быть реализована, как представлено на рис. 4.

В отличие от обычного L-BP-декодера, память, хранящая значения апостериорных LLR Λ_i, инициализируется непереставленными подвекторами входных LLR λ_i. Памяти апостериорных LLR разбиты на группы по γ элементов в каждой. Пусть при этом эти группы перенумерованы и $p = 1, ..., \gamma/\rho$ — номер группы. После обработки одной полосы, в отличие от обычного декодера L-BP, обновленные векторы $\Lambda_{(p-1)\gamma+i}$ попадают не в память с номером $(p-1)\gamma + i$, а в память с номером $(((p-1)\gamma + i) \bmod \gamma) + 1$, т. е. перед записью в память циклически сдвигаются. Каждый блок памяти внутри группы соединен с фиксированной перестановкой из первой полосы матрицы **H**. После обработки первой полосы векторы Λ_i будут размещены в блоках памяти так, что при обработке следующей полосы подвергнутся нужной фиксированной перестановке, так как следующая полоса в макроблоке является циклическим сдвигом предыдущей.



■ ***Рис. 4.*** Частично параллельная архитектура декодера L-BP для кода с циклической структурой макроблоков

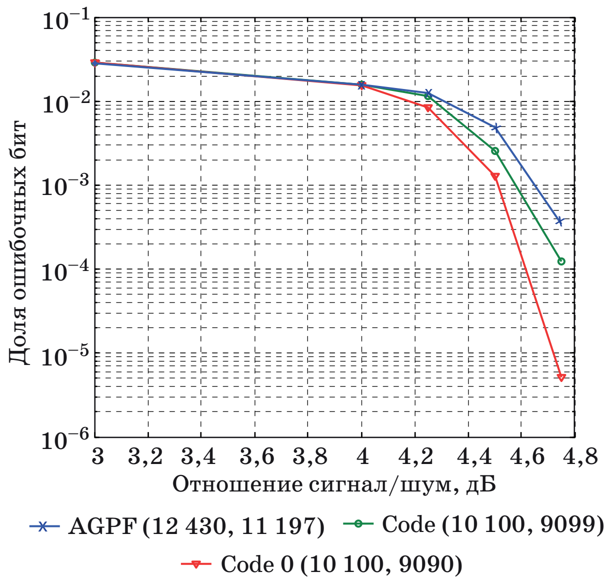
Пусть, например, $\gamma = 3$ и макроблок содержит блоки — матрицы перестановок **A**, **B** и **C**. В начале обработки векторы Λ_1, Λ_2, Λ_3 находятся в 1-, 2-, 3-м блоках памяти соответственно. При обработке первой полосы векторы Λ_1, Λ_2, Λ_3 подвергаются перестановкам **A**, **B**, **C** соответственно. После обработки FH-VNP-, CNP- и SH-VNP-процессорами происходит обратная перестановка, а затем Λ_1, Λ_2, Λ_3 попадают во 2-, 3- и 1-й блок памяти соответственно. Таким образом, при обработке следующей полосы Λ_1, Λ_2, Λ_3 подвергнутся перестановкам **C**, **A**, **B** соответственно. После обработки всех полос векторы Λ_1, Λ_2, Λ_3 окажутся в исходных блоках памяти.

Результаты моделирования

Проведем анализ результатов моделирования рассмотренных конструкций в канале с АБГШ. Так как основное преимущество предложенных модификаций — эффективность реализации в высокоскоростных системах передачи информации, выберем высокоскоростной код, например $R = 0{,}9$ с длиной порядка 10 000. Такие параметры соответствуют, к примеру, кодовым схемам передачи по оптоволоконным линиям [4, 8]. В качестве кода для сравнения выберем конструкцию, основанную на аддитивной группе конечного поля (additive group of prime field — AGPF) [25].

Для построения кода с циклической структурой макроблоков выберем поле GF(101), $\gamma = 10$. Так как 101 — простое число, блоки проверочной матрицы представляют собой циклические перестановки, и полученный код является квазициклическим, с длиной 10 100 и количеством информационных символов 9099. Заменив диагонали макроблоков нулевыми блоками, получим квазициклический код с длиной 10 100 и количеством информационных символов 9090. Заметим, что в этом случае проверочная матрица имеет полный ранг, что может быть использовано для более эффективной процедуры кодирования [11, 29].

Результаты моделирования в канале с АБГШ приведены на рис. 5. Был использован декодер распространения доверия с 30 итерациями. Код из работы [25] обозначен как «AGPF», код



■ ***Рис. 5.*** Результаты моделирования в канале с АБГШ

с циклической структурой макроблоков — как «Code», а код с маскированием нулевыми блоками — как «Code 0». Видно, что коды с циклической структурой макроблоков превосходят код AGPF при выбранных параметрах по вероятности ошибки на информационный бит, а добавление нулевых блоков дает эффект за счет улучшения цикловой структуры графа Таннера. Вместе с этим предложенные коды позволяют построение более эффективных архитектур декодирования.

Заключение

В статье рассмотрена модификация комбинаторной конструкции кодов с малой плотностью проверок на четность, основанной на кодах Рида — Соломона, которая позволяет получать проверочную матрицу кода, обладающую свойством циклической структуры макроблоков. Для данной конструкции проведено моделирование в канале с АБГШ.

Предложен вариант частично параллельной архитектуры декодера L-BP, использующей только фиксированные перестановки за счет наличия циклической структуры макроблоков в проверочной матрице кода. Это позволяет упростить декодирование.

Литература

1. **Gallager R. G.** Low-Density Parity-Check Codes // IRE Transactions on Information Theory. Jan. 1962. Vol. 8. N 1. P. 21–28. doi:10.1109/TIT.1962.1057683
2. **Gallager R. G.** Low Density Parity Check Codes. — Cambridge, MA: MIT Press, 1963. — 90 p.
3. **Krouk E., Semenov S.,** et al. Modulation and Coding Techniques in Wireless Communications/Ed. by E. Krouk, S. Semenov. — John Wiley & Sons, 2011. — 680 p. doi:10.1002/9780470976777
4. **Djordjevic I., Ryan W., and Vasic B.** Coding for Optical Channels. — Springer, 2010. — 444 p. doi:10.1007/978-1-4419-5569-2
5. IEEE 802.3an-2006. Part 3: CSMA/CD Access Method and Physical Layer Specifications — Amendment: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T. Oct. 2006. http://www.techstreet.com/standards/ieee-802-3an-2006?product_id=1514965 (дата обращения: 25.01.2017).
6. IEEE 802.16e-2005. Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. Feb. 2006. http://www.techstreet.com/standards/ieee-802-16e-2005?product_id=1270606 (дата обращения: 25.01.2017).
7. IEEE 802.11n/d1.0. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Mar. 2006. http://www.techstreet.com/standards/ieee-802-16e-2005?product_id=1270606 (дата обращения: 25.01.2017).
8. ITU-T Recommendation G.975.1. Forward Error Correction for High Bit Rate DWDM Submarine Systems. Feb. 2004. https://www.itu.int/rec/T-REC-G.975.1-200402-I/en (дата обращения: 25.01.2017).
9. **Zyablov V. V., Pinsker M. S.** Estimation of the Error-Correction Complexity for Gallager Low-Density Codes // Problems of Information Transmission. 1975. Vol. 11. N 1. P. 23–36.
10. **Tanner R.** A Recursive Approach to Low Complexity Codes // IEEE Transactions on Information Theory. Sept. 1981. Vol. 27. N 5. P. 533–547. doi:10.1109/TIT.1981.1056404
11. **Lin S., Ryan W.** Channel Codes: Classical and Modern. — Cambridge University Press, 2009. — 710 p.
12. **Richardson T. J., Urbanke R. L.** The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding // IEEE Transactions on Information Theory. Feb. 2001. Vol. 47. N 2. P. 599–618. doi:10.1109/18.910577
13. **Chung S.-Y., Forney G. D., Richardson T. J., Urbanke R.** On the Design of Low-Density Parity-Check Codes Within 0.0045 dB of the Shannon Limit // IEEE Communications Letters. Feb. 2001. Vol. 5. N 2. P. 58–60. doi:10.1109/4234.905935
14. **Richardson T. J., Shokrollahi M. A., Urbanke R. L.** Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes // IEEE Transactions on Information Theory. Feb. 2001. Vol. 47. N 2. P. 619–637. doi:10.1109/18.910578
15. **Di C., Proietti D., Teletar I. E., Richardson T. J., Urbanke R. L.** Finite Length Analysis of Low-Density

Parity-Check Codes on the Binary Erasure Channels // IEEE Transactions on Information Theory. Jun. 2002. Vol. 48. N 6. P. 1570–1579. doi:10.1109/TIT.2002.1003839
16. **Richardson T.** Error Floors of LDPC Codes // Proc. 41st Allerton Conf. on Communications, Control, and Computing. Allerton House, IL, Oct. 2003. http://web.stanford.edu/class/ee388/papers/ErrorFloors.pdf (дата обращения: 25.01.2017).
17. **Козлов А. В., Крук Е. А., Овчинников А. А.** Подход к построению блочно-перестановочных кодов с малой плотностью проверок на четность // Изв. вузов. Приборостроение. 2013. Т. 56. № 8. С. 9–14.
18. **Kschischang F. R., Frey B. J., Loeliger H. A.** Factor Graphs and the Sum-Product Algorithm // IEEE Transactions on Information Theory. Feb. 2001. Vol. 47. N 2. P. 498–519. doi:10.1109/18.910572
19. **Zhang J., Fossorier M. P. C.** Shuffled Iterative Decoding // IEEE Transactions on Communications. Feb. 2005. Vol. 53. N 2. P. 209–213. doi:10.1109/TCOMM.2004.841982
20. **Park I.-C., Kang S.-H.** Scheduling Algorithm for Partially Parallel Architecture of LDPC Decoder by Matrix Permutation // 2005 IEEE International Symposium on Circuits and Systems. 2005. Vol. 6. P. 5778–5781. doi:10.1109/ISCAS.2005.1465951
21. **Yamagishi H., Noda M.** High Throughput Hardware Architecture for (1440,1344) Low-Density Parity-Check Code Utilizing Quasi-Cyclic Structure // 2008 5th Intern. Symp. on Turbo Codes and Related Topics. Lausanne, 2008. P. 78–83. doi:10.1109/TURBOCODING.2008.4658676
22. **Mansour M. M., Shanbhag N. R.** High-Throughput LDPC Decoders // IEEE Transactions on Very Large Scale Integration (VLSI) Systems. Dec. 2003. Vol. 11. N 6. P. 976–996. doi:10.1109/TVLSI.2003.817545
23. **Hocevar D. E.** A Reduced Complexity Decoder Architecture Via Layered Decoding of LDPC Codes // IEEE Workshop on Signal Processing Systems. 2004. SIPS 2004. Austin, TX. P. 107–112. doi:10.1109/SIPS.2004.1363033
24. **Diao Q., Huang Q., Lin S., Abdel-Ghaffar K.** A Matrix-Theoretic Approach for Analyzing Quasi-Cyclic Low-Density Parity-Check Codes // IEEE Transactions on Information Theory. Jun. 2012. Vol. 58. N 6. P. 4030–4048. doi:10.1109/TIT.2012.2184834
25. **Lan L., Zeng L., Tai Y. Y., Chen L., Lin S., Abdel-Ghaffar K.** Construction of Quasi-Cyclic LDPC Codes for AWGN and Binary Erasure Channels: A Finite Field Approach // IEEE Transactions on Information Theory. Jul. 2007. Vol. 53. N 7. P. 2429–2458. doi:10.1109/TIT.2007.899516
26. **Djurdjevic I., Xu J., Abdel-Ghaffar K., Lin S.** A Class of Low-Density Parity-Check Codes Constructed Based on Reed–Solomon Codes with Two Information Symbols // IEEE Communications Letters. Jul. 2003. Vol. 7. N 7. P. 317–319. doi:10.1109/LCOMM.2003.814716
27. **MacWilliams F., Sloane N.** The Theory of Error-Correcting Codes. — North-Holland publishing company, 1983. — 782 p.
28. **Kabatiansky G., Semenov S., Krouk E.** Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept. — John Wiley & Sons, 2005. — 278 p. doi:10.1002/0470867574
29. **Li Z., Chen L., Zeng L., Lin S., Fong W. H.** Efficient Encoding of Quasi-Cyclic Low-Density Parity-Check Codes // IEEE Transactions on Communications. Jan. 2006. Vol. 54. N 1. P. 71–81. doi:10.1109/TCOMM.2005.861667

UDC 621.391.251
doi:10.15217/issn1684-8853.2017.2.58

Low-Density Parity-Check Codes with Cyclic Structure of Macroblocks

Ivanov D. O.[a], Programmer Engineer, denis.ivo@vu.spb.ru
Kozlov A. V.[a], Senior Programmer Engineer, akozlov@vu.spb.ru
Ovchinnikov A. A.[a], PhD, Tech., Associate Professor, mldoc@vu.spb.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Modern infocommunication systems require a very high rate of data transmission with high reliability, i.e. low probability of an error. To fight the distortions in a communication channel, error-correcting codes are traditionally used. Low-density parity-check codes are one of the most powerful and effective modern error-correcting techniques. However, to attain a high rate of the transmission, it is not enough to use codes which only correct errors and have simple encoding/decoding procedures. The very construction of the codes should facilitate a more effective implementation, including the hardware level. **Purpose:** The goal is to construct effective low-density parity-check codes whose structure would allow you to optimize the existing decoder architectures. **Results:** A modification of low-density parity-check code has been proposed, based on Reed-Solomon codes. It has a cyclic structure of macroblocks. It is shown how this structure can be used to optimize the architecture of a partially parallel decoder based on a layered belief propagation algorithm. **Practical relevance:** The proposed code construction and decoder architecture allow you to achieve low error probabilities in high-rate data communication systems (e.g. optical wired lines).

Keywords — Low-Density Parity-Check Codes, Codes with Cyclic Structure of Macroblocks, Layered Belief Propagation Algorithm, Partially Parallel Decoding Architecture.

References

1. Gallager R. G. Low-Density Parity-Check Codes. *IRE Transactions on Information Theory*, Jan. 1962, vol. 8, no. 1, pp. 21–28. doi:10.1109/TIT.1962.1057683
2. Gallager R. G. *Low Density Parity Check Codes*. Cambridge, MA, MIT Press, 1963. 90 p.
3. Krouk E., Semenov S., et al. *Modulation and Coding Techniques in Wireless Communications*. Ed. by E. Krouk, S. Semenov. John Wiley & Sons, 2011. 680 p. doi:10.1002/9780470976777
4. Djordjevic I., Ryan W., and Vasic B. *Coding for Optical Channels*. Springer, 2010. 444 p. doi:10.1007/978-1-4419-5569-2
5. *IEEE 802.3an-2006. Part 3: CSMA/CD Access Method and Physical Layer Specifications — Amendment: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T*. Oct. 2006. Available at: http://standards.ieee.org/getieee802/download/802.3-2015.zip (accessed 25 January 2017).
6. *IEEE 802.16e-2005. Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems*. Feb. 2006. Available at: http://standards.ieee.org/getieee802/download/802.16e-2005.pdf (accessed 25 January 2017).
7. *IEEE 802.11n/d1.0. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Mar. 2006. Available at: http://standards.ieee.org/getieee802/download/802.11-2012.pdf (accessed 25 January 2017).
8. *ITU-T Recommendation G.975.1. Forward Error Correction for High Bit Rate DWDM Submarine Systems*. Feb. 2004. Available at: *https://www.itu.int/rec/T-REC-G.975.1-200402-I/en* (accessed 25 January 2017).
9. Zyablov V. V., Pinsker M. S. Estimation of the Error-Correction Complexity for Gallager Low-Density Codes. *Problems of Information Transmission*, 1975, vol. 11, no. 1, pp. 23–36.
10. Tanner R. A Recursive Approach to Low Complexity Codes. *IEEE Transactions on Information Theory*, Sept. 1981, vol. 27, no. 5, pp. 533–547. doi:10.1109/TIT.1981.1056404
11. Lin S., Ryan W. *Channel Codes: Classical and Modern*. Cambridge University Press, 2009. 710 p.
12. Richardson T. J., Urbanke R. L. The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding. *IEEE Transactions on Information Theory*, Feb. 2001, vol. 47, no. 2, pp. 599–618. doi:10.1109/18.910577
13. Chung S.-Y., Forney G. D., Richardson T. J., Urbanke R. On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit. *IEEE Communications Letters*, Feb. 2001, vol. 5, no. 2, pp. 58–60. doi:10.1109/4234.905935
14. Richardson T. J., Shokrollahi M. A., Urbanke R. L. Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes. *IEEE Transactions on Information Theory*, Feb. 2001, vol. 47, no. 2, pp. 619–637. doi:10.1109/18.910578
15. Di C., Proietti D., Teletar I. E., Richardson T. J., Urbanke R. L. Finite Length Analysis of Low-Density Parity-Check Codes on the Binary Erasure Channels. *IEEE Transactions on Information Theory*, Jun. 2002, vol. 48, no. 6, pp. 1570–1579. doi:10.1109/TIT.2002.1003839
16. Richardson T. Error Floors of LDPC Codes. *Proc. 41st Allerton Conf. on Communications, Control, and Computing*, Monticello, IL, Oct. 2003. http://web.stanford.edu/class/ee388/papers/ErrorFloors.pdf (accessed 25 January 2017).
17. Kozlov A., Krouk E., Ovchinnikov A. An Approach to Development of Block-Commutative Codes with Low Density of Parity Check. *Izvestiia vuzov. Priborostroenie*, 2013, vol. 8, pp. 9–14 (In Russian).
18. Kschischang F. R., Frey B. J., Loeliger H. A. Factor Graphs and the Sum-Product Algorithm. *IEEE Transactions on Information Theory*, Feb. 2001, vol. 47, no. 2, pp. 498–519. doi:10.1109/18.910572
19. Zhang J., Fossorier M. P. C. Shuffled Iterative Decoding. *IEEE Transactions on Communications*, Feb. 2005, vol. 53, no. 2, pp. 209–213. doi:10.1109/TCOMM.2004.841982
20. Park I.-C., Kang S.-H. Scheduling Algorithm for Partially Parallel Architecture of LDPC Decoder by Matrix Permutation. *2005 IEEE Intern. Symp. on Circuits and Systems*, 2005, vol. 6, pp. 5778–5781. doi:10.1109/ISCAS.2005.1465951
21. Yamagishi H., Noda M. High Throughput Hardware Architecture for (1440,1344) Low-Density Parity-Check Code Utilizing Quasi-Cyclic Structure. *2008 5th Intern. Symp. on Turbo Codes and Related Topics*, Lausanne, 2008, pp. 78–83. doi:10.1109/TURBOCODING.2008.4658676
22. Mansour M. M., Shanbhag N. R. High-throughput LDPC Decoders. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Dec. 2003, vol. 11, no. 6, pp. 976–996. doi:10.1109/TVLSI.2003.817545
23. Hocevar D. E. A Reduced Complexity Decoder Architecture Via Layered Decoding of LDPC Codes. *IEEE Workshop on Signal Processing Systems*, 2004, SIPS 2004, Austin, TX, pp. 107–112. doi:10.1109/SIPS.2004.1363033
24. Diao Q., Huang Q., Lin S., Abdel-Ghaffar K. A Matrix-Theoretic Approach for Analyzing Quasi-Cyclic Low-Density Parity-Check Codes. *IEEE Transactions on Information Theory*, Jun. 2012, vol. 58, no. 6, pp. 4030–4048. doi:10.1109/TIT.2012.2184834
25. Lan L., Zeng L., Tai Y. Y., Chen L., Lin S., Abdel-Ghaffar K. Construction of Quasi-Cyclic LDPC Codes for AWGN and Binary Erasure Channels: A Finite Field Approach. *IEEE Transactions on Information Theory*, Jul. 2007, vol. 53, no. 7, pp. 2429–2458. doi:10.1109/TIT.2007.899516
26. Djurdjevic I., Xu J., Abdel-Ghaffar K., Lin S. A Class of Low-Density Parity-Check Codes Constructed Based on Reed-Solomon Codes with Two Information Symbols. *IEEE Communications Letters*, Jul. 2003, vol. 7, no. 7, pp. 317–319. doi:10.1109/LCOMM.2003.814716
27. MacWilliams F., Sloane N. *The Theory of Error-Correcting Codes*. North-Holland publishing company, 1983. 782 p.
28. Kabatiansky G., Semenov S., Krouk E. *Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept*. John Wiley & Sons, 2005. 278 p. doi:10.1002/0470867574
29. Li Z., Chen L., Zeng L., Lin S., Fong W. H. Efficient Encoding of Quasi-Cyclic Low-Density Parity-Check Codes. *IEEE Transactions on Communications*, Jan. 2006, vol. 54, no. 1, pp. 71–81. doi:10.1109/TCOMM.2005.861667