

МЕТОДЫ И АППАРАТУРА КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ НИЗКОПЛОТНОСТНЫХ КВАЗИЦИКЛИЧЕСКИХ КОДОВ

Кравченко А.Н., к.т.н., проектировщик систем Ubiso GmbH, Germany, e-mail: alexander.kravtchenko@ubiso.com

Ключевые слова: кодирование, декодирование, низкоплотностное, LDPC коды, проверочная матрица, кодовая скорость.

Введение

Системы связи и вещания, в частности беспроводные системы, часто подвержены помехам, в связи с чем использование помехоустойчивых кодов имеет важное значение. Среди помехоустойчивых кодов LDPC коды, предложенные Галлагером [1] и позже вновь открытые Маккеем и Нилом [2], появляются как класс кодов, которые обладают эффективной способностью исправлять ошибки в каналах связи. Превосходная эффективность декодирования этих кодов получается при использовании алгоритма декодирования, вычисляющего итеративно распределение вероятностей в граф-ориентированной модели, который известен в литературе как «belief propagation algorithm» (BPA). В отечественной литературе этот метод известен как алгоритм декодирования с итеративным распространением доверия (АРД) [3]. Следует отметить, что в литературе существует большое количество модификаций этого алгоритма (алгоритмы, основывающиеся на логарифмическом отношении функций правдоподобия, упрощенные методы). Некоторые сведения о модификациях можно найти в [11]. В настоящее время LDPC коды со средней пропускной способностью используются в стандартах как DVB-S2, WiMax(IEEE 802.16e) и WLAN(IEEE 802.11n). Более того, LDPC коды с высокой пропускной способностью используются в стандарте WPAN (IEEE 802.15.3c). Следует отметить, что во всех перечисленных стандартах используются квази-циклические низкоплотностные коды (QC-LDPC).

QC-LDPC коды, основные определения

LDPC коды универсально специфицируются их проверочными матрицами. Проверочная матрица QC-LDPC кода задается как массив циркулянтов (перестановочных матриц) одного и того же размера. Циркулянт [4] представляет собой квадратную матрицу $(b \times b)$, в которой каждая последующая строка является циклическим сдвигом вправо на одно место предыдущей строки. Индекс сдвига определяет позицию «1» в первой строке матрицы. Весы строк и столбцов в циркулянте одни и те же, скажем к примеру $w = 1$. Для простоты можно сказать, что циркулянт имеет вес Хэмминга w . Если $w = 1$, то циркулянт есть циклическая перестановочная матрица. Циркулянт полностью характеризуется его первой стро-

Произведен анализ проверочных матриц нерегулярных квазициклических низкоплотностных кодов WPAN (IEEE 802.15.3c) стандарта (QC-LDPC). Установлено, что проверочные матрицы являются квадратичными и обратимыми. В связи с этим к расчету порождающих матриц применен традиционный метод с приложением к квазициклическим низкоплотностным кодам. Приведены методы кодирования и декодирования QC-LDPC кодов на основе проверочных матриц. Предложена аппаратура кодирования этих кодов. Представлены результаты моделирования эффективности декодирования LDPC кодов WPAN-стандарта в канале с АБГШ для случая двоичной фазовой модуляции.

кой (или первым столбцом), которую называют генератором циркулянта. LDPC код определяется матрицей размера $n \times m$, где n длина кода и m число проверочных бит в коде. Число информационных бит определяется как $k = n - m$. Проверочная матрица \mathbf{H}_{qc} QC-LDPC кода с размерностью $t \times c$, где $n = b \times t$ и $m = b \times c$, может быть построена путем соединения $t \times c$ циклических перестановочных матриц размерности $(b \times b)$.

Матрица \mathbf{H}_{qc} QC-LDPC кода для двух натуральных чисел t и c с $c \leq t$ может быть определена как массив циркулянтов $\mathbf{A}_{i,j}$ в поле $GF(2)$:

$$\mathbf{H}_{qc} = \begin{bmatrix} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \cdots & \mathbf{A}_{1,t} \\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \cdots & \mathbf{A}_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{c,1} & \mathbf{A}_{c,2} & \cdots & \mathbf{A}_{c,t} \end{bmatrix} \quad (1)$$

Структуру QC-LDPC кода можно определить на основе его проверочной матрицы в циркулянтной форме, определенной формулой (1). На основе этой формы, каждая кодовая строка \mathbf{v} может быть разделена на секции $\mathbf{v} = (v_1, v_2, \dots, v_t)$, и каждая секция v_j включает b компонент (бит). Для $1 \leq j \leq t$, b компонент j -ой секции соответствуют b столбам j -го столбца циркулянта в \mathbf{H}_{qc} .

Анализ проверочных матриц и метод кодирования

LDPC коды, используемые в системе WPAN [5], являются систематическими нерегулярными QC-LDPC кодами. Табл. 1 для примера иллюстрирует проверочную матрицу LDPC кода с кодовой скоростью $R = 7/8$.

Индекс -1 определяет нулевую перестановочную матрицу (матрица состоит из одних нулей). Проверочная матрица состоит из двух частей $\mathbf{H}_{qc} = [\mathbf{H}_1 \mathbf{H}_2]$, где \mathbf{H}_1 субматрица соответствует информационным битам, и \mathbf{H}_2 представляет проверочные биты кодового слова. Кодовое слово должно удовлетворять уравнению $\mathbf{H}_{qc} \cdot \mathbf{v}^T = 0$.

Таблица 1. Проверочная матрица LDPC кода с кодовой скоростью R = 7/8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	18	6	5	7	18	16	0	10	2	3	6	10	16	9	0	20	7	9	5	4	12	4	4	4	10	19	5	10	-1	-1	-1
5	0	18	6	0	7	18	16	6	10	2	3	0	10	16	9	5	20	7	9	4	4	12	4	5	4	10	19	19	10	-1	-1
6	5	0	18	16	0	7	18	3	6	10	2	9	0	10	16	9	5	20	7	4	4	4	12	19	5	4	10	17	19	10	-1
18	6	5	0	18	16	0	7	2	3	6	10	16	9	0	10	7	9	5	20	12	4	4	4	10	19	5	4	7	17	19	10

Анализ проверочных матриц всех кодов показывает, что \mathbf{H}_2 - части матриц \mathbf{H}_{gc} квадратичны и обратимы, в том числе и для LDPC кода с R=7/8. В этом случае для расчета порождающей матрицы \mathbf{G}_{gc} может быть использован традиционный метод [6] с применением к QC-LDPC кодам. Исходя из этого, субматрицу \mathbf{H}_2 можно представить в виде

$$\mathbf{H}_2 = \begin{bmatrix} \mathbf{A}_{1,t-c+1} & \mathbf{A}_{1,t-c+2} & \dots & \mathbf{A}_{1,t} \\ \mathbf{A}_{2,t-c+1} & \mathbf{A}_{2,t-c+2} & \dots & \mathbf{A}_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{c,t-c+1} & \mathbf{A}_{c,t-c+2} & \dots & \mathbf{A}_{c,t} \end{bmatrix} \quad (2)$$

Порождающая матрица может быть представлена как

$$\mathbf{G}_{gc} = \begin{bmatrix} \mathbf{G}_1 \\ \mathbf{G}_2 \\ \vdots \\ \mathbf{G}_{t-c} \end{bmatrix} = \begin{bmatrix} \mathbf{I} & \mathbf{O} & \dots & \mathbf{O} & \mathbf{G}_{1,1} & \mathbf{G}_{1,2} & \dots & \mathbf{G}_{1,c} \\ \vdots & \mathbf{I} & \dots & \mathbf{O} & \mathbf{G}_{2,1} & \mathbf{G}_{2,2} & \dots & \mathbf{G}_{2,c} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \dots & \mathbf{I} & \mathbf{G}_{t-c,1} & \mathbf{G}_{t-c,2} & \dots & \mathbf{G}_{t-c,c} \end{bmatrix} = \begin{bmatrix} \mathbf{I}_{(t-c)b} & \mathbf{P} \end{bmatrix} \quad (3)$$

где \mathbf{I} - единичная матрица размерности $b \times b$, \mathbf{O} - нулевая матрица размерности $b \times b$ и $\mathbf{G}_{i,j}$ - циркулянты с $1 \leq i \leq t-c$ и $1 \leq j \leq c$ и размерностью $b \times b$.

Порождающая матрица (3) состоит из двух частей: левой части $\mathbf{I}_{(t-c)b}$ и правой части \mathbf{P} . Левая часть матрицы $\mathbf{I}_{(t-c)b}$ с $(t-c)b \times (t-c)b$ представляет собой единичные матрицы, расположенные на главной диагонали, а правая часть - массив циркулянтов. Представление кода в форме (3) является систематическим представлением [6]. Левая часть отображает информационные биты кодового слова, правая часть - его проверочные биты. Необходимым и достаточным условием для существования порождающей матрицы \mathbf{G}_{gc} является условие $\mathbf{H}_{gc} \mathbf{G}_{gc}^T = \mathbf{O}$. Допустим $\mathbf{g}_{i,j}$ представляет собой генератор циркулянта $\mathbf{G}_{i,j}$. Когда $\mathbf{g}_{i,j}$ известны, можно сформировать все циркулянты порождающей матрицы \mathbf{G}_{gc} .

Таким образом \mathbf{G}_{gc} характеризуется полностью группой $c(t-c)$ генераторов. Допустим $\mathbf{u} = (1, 0, \dots, 0)$ есть группа из b бит с '1' в первой позиции и $\mathbf{0} = (0, 0, \dots, 0)$ - группа, которая содержит только нули. Для $1 \leq i \leq t-c$ первый ряд субматрицы \mathbf{G}_i определяется следующим образом

$$\mathbf{g}_i = (\mathbf{0} \dots \mathbf{0} \mathbf{u} \mathbf{0} \dots \mathbf{0} \mathbf{g}_{i,1} \mathbf{g}_{i,2} \dots \mathbf{g}_{i,c}), \quad (4)$$

где группа \mathbf{u} находится в i -ой позиции \mathbf{g}_i .

Обозначим $\mathbf{z}_i = (\mathbf{g}_{i,1} \mathbf{g}_{i,2} \dots \mathbf{g}_{i,c})$ и $\mathbf{H}_1^{(i)} = [\mathbf{A}_{1,i}^T \dots \mathbf{A}_{c,i}^T]^T$. Тогда выражение $\mathbf{H}_{gc} \mathbf{g}_i^T = \mathbf{0}$ дает следующее равенство:

$$\mathbf{H}_1^{(i)} \mathbf{u}^T + \mathbf{H}_2 \mathbf{z}_i^T = \mathbf{0}. \quad (5)$$

Поскольку \mathbf{H}_2 есть квадратная матрица и имеет полный ранг, то она обратима. Тогда из (5) следует

$$\mathbf{z}_i^T = \mathbf{H}_2^{-1} \mathbf{H}_1^{(i)} \mathbf{u}^T. \quad (6)$$

Решение (6) для $1 \leq i \leq t-c$ дает все генераторы $\mathbf{g}_{i,j}$ порождающей матрицы \mathbf{G}_{gc} .

Обозначим $\mathbf{a} = (a_1, a_2, \dots, a_{(t-c)b})$ как информационную последовательность бит $(t-c)b$, подлежащих кодированию. После деления информационных бит на секции $(t-c)$ равной длины $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{t-c})$, кодовое слово можно представить в форме $\mathbf{v} = \mathbf{a} \mathbf{G}_{gc}$, которое имеет систематическое представление: $\mathbf{v} = (\mathbf{a}, \mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_c)$. Здесь $\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_c$ - секции равной длины b , где каждая секция представляет собой проверочные биты $\mathbf{p}_j = (p_{j,1}, p_{j,2}, \dots, p_{j,b})$. Проверочные биты в каждой секции вычисляются в соответствии с выражением

$$\mathbf{p}_j = \mathbf{a}_1 \mathbf{G}_{1,j} + \mathbf{a}_2 \mathbf{G}_{2,j} + \dots + \mathbf{a}_{t-c} \mathbf{G}_{t-c,j}. \quad (7)$$

На основании рассмотренного метода были вычислены генераторы для всех порождающих матриц стандарта. Например, рис. 1 иллюстрирует генераторы, вычисленные для LDPC кода с кодовой скоростью R=7/8.

0	000200	000011	01100c	048088	14	000001	005000	104028	028a88
1	001000	000208	008031	01904c	15	000200	000000	004004	105020
2	000008	009000	020248	048071	16	000400	000012	012009	043094
3	000010	010008	049080	0a02c8	17	000004	004400	010032	032029
4	000004	004200	014021	020004	18	000001	001004	000408	01803a
5	001000	00000c	00c220	01c061	19	000010	010001	041084	080488
6	004000	001020	02008c	02c320	20	000020	020020	0a0120	1e0000
7	000200	004001	000024	021084	21	040000	000220	020821	0a1121
8	100000	000808	00a044	0640c4	22	000020	060000	080320	120921
9	000080	180000	000c09	00a446	23	000020	020020	0e0100	180220
10	000040	040080	080200	000e08	24	000020	020010	090900	040184
11	000008	008040	0600c0	0c0240	25	100000	000820	022014	094904
12	100000	000a00	002004	000000	26	000800	100004	004830	026034
13	004000	100020	020a80	022104	27	000010	010800	140084	0848b0

Рис. 1. Генераторы порождающей матрицы для LDPC кода с R=7/8

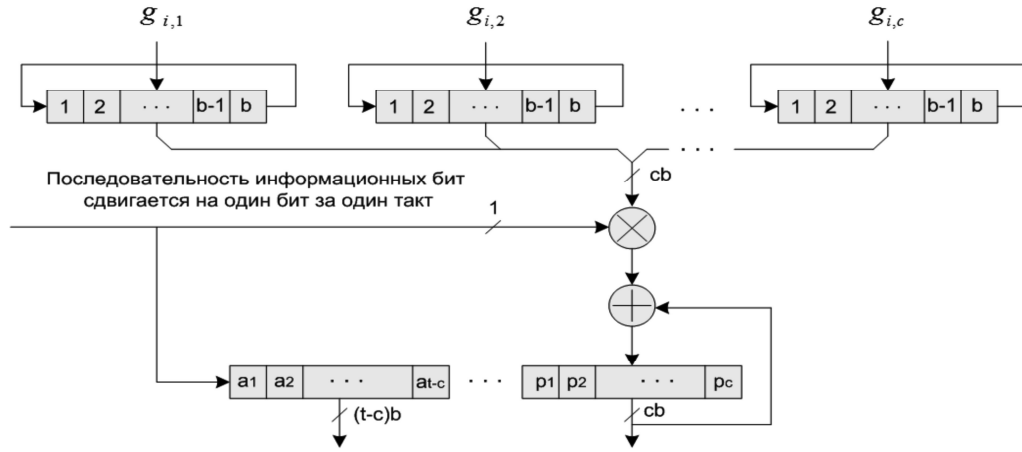


Рис. 2. Структура кодера

Представление G_{qc} в виде генераторов очень практично при разработке аппаратуры. В основе кодера лежит циклический сдвигающий регистр, который первоначально загружается генератором и в процессе последовательных сдвигов реализует циркулянт. Рис. 2 представляет структуру кодера. Кодер передает информационные биты на выход, как биты кодового слова. Одновременно кодер вычисляет проверочные биты $p_j = (p_{j,1}, p_{j,2}, \dots, p_{j,b})$ путем последовательного выполнения умножения циркулянтов на группы информационных бит. Непосредственное осуществление матричного умножения показано на рис. 2, как это предлагает Лин [7].

Циклические сдвигающие регистры, каждый длины b , загружаются генераторами (первая строка рис. 1). Для каждого информационного бита a_m ($m = 1, \dots, (t-c)b$), в свою очередь, эти регистры циклически сдвигаются один раз. Если $a_m = 1$, то выполняется операция XOR и результат загружается в выходной регистр (проверочные биты). Когда операция перемножения циркулянтов на информационные биты группы завершена, следующие генераторы $g_{1,1}, g_{1,2}, \dots, g_{1,c}$ загружаются в регистры сдвига, и операция кодирования повторяется. Процесс кодирования завершается, когда последняя группа циркулянтов (27, рис. 1) перемножается на последнюю группу информационных бит (27). После кодирования все проверочные биты находятся в выходном регистре.

Декодирование QC-LDPC кодов

Для декодирования QC-LDPC кодов широко используется алгоритм послойного декодирования (layered decoding), развитый в работах [8-9]. Применение этого алгоритма для декодирования кодов в стандартах DVB-S2, WiMax(IEEE 802.16e) и WLAN(IEEE 802.11n) изложено в работе [10]. В настоящей работе этот алгоритм применен для декодирования кодов стандарта WPAN (IEEE 802.15.3c). Коротко остановимся на особенностях алгоритма:

1. Декодер, спроектированный при использовании этого алгоритма, требует меньшего объема памяти чем стандартный декодер, реализующий стандартный двух-фазный метод декодирования – «сумма произведение» (two-phase message-passing, TPMP algorithm) [10].

2. Скорость сходимости алгоритма существенно выше чем у «TPMP» (алгоритм выполняет меньше итераций

для достижения равной эффективности декодирования).

При описании алгоритма воспользуемся метрикой, называемой логарифмическим отношением функций правдоподобия (log-likelihood ratio - LLR), которая определяется выражением

$$LLR(x | y) = \ln \left[\frac{p(y | x = 0)}{p(y | x = 1)} \right].$$

Допустим, $x = [x_1, x_2, \dots, x_n]$ обозначает кодовое слово, которое модулируется при использовании двоичной фазовой модуляции, и модулированные значения x передаются по каналу с белым аддитивным гауссовым шумом (АБГШ). Допустим $y = [y_1, y_2, \dots, y_n]$ обозначает входную последовательность принятых сигналов (символов). Демодулятор принимает входную последовательность сигналов и вычисляет соответствующие LLR значения для: $j = 1, 2, \dots, n$

$$\lambda_j = LLR(y_j | x_j) = \ln \left[\frac{p(y_j | x_j = 0)}{p(y_j | x_j = 1)} \right]. \quad (8)$$

Обычно при двоичной bipolarной передаче по каналу LLR значения вычисляются как

$$\lambda_j = \frac{2}{\sigma^2} * y_j \quad (9)$$

где σ^2 - дисперсия АБГШ.

При описании алгоритма воспользуемся следующими обозначениями:

λ_j - «LLR» значение принятого j -го символа, $R_y[k]$ – внешние (extrinsic) «LLR» значения, $Q_y[k]$ – внутренние (intrinsic) «LLR» значения, Λ_j - апостериорные «LLR» значения.

Выполнение алгоритма осуществляется в следующем порядке:

1. Инициализация:

$$R_y^0 = 0, \Lambda_j^0 = \lambda_j. \quad (10)$$

2. Горизонтальное сканирование (check node update rule):

$$Q_{ji}^{(k)} = \Lambda_j^{(k-1)} - R_y^{(k-1)}; \quad (11)$$

$$R_y^{(k)} = \prod_{j \in R\{i\} \setminus j} \text{sign}(Q_{ji}^{(k)}) * \{ \text{MIN}_{j \in R\{i\} \setminus j} | Q_{ji}^{(k)} | \}; \quad (12)$$

$$\Lambda_j^{(k)} = Q_{ji}^{(k)} + R_y^{(k)}, \quad (13)$$

где k – текущая итерация.

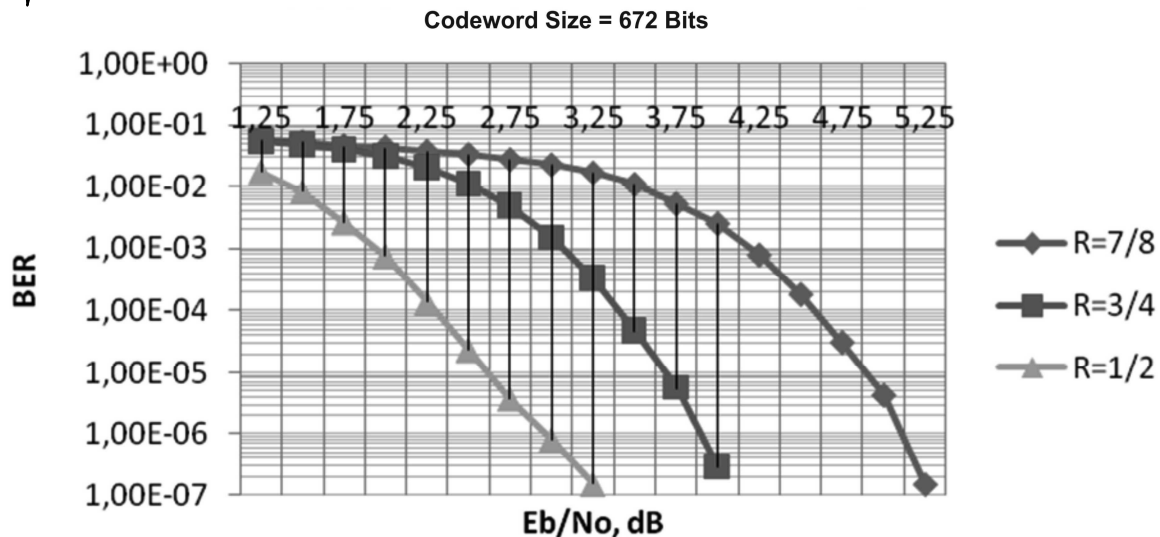


Рис. 3. Эффективность декодера для кодовых скоростей – 1/2, 3/4, 7/8

Твердое решение декодера (hard decision) после каждой итерации осуществляется на основе проверки условия - $v = 1$, если $\Lambda_j^{(k)} \leq 0$, иначе $v = 0$.

Шаг 2 выполняется до тех пор, пока не выполнится условие - $\mathbf{H}_{qc} \cdot \mathbf{v}^T = 0$ или будет достигнуто максимальное значение итераций. При вычислении $R_y[k]$ используется метод, основанный на минималии сумме (*Min-sum* - аппроксимация) [11]. Данный алгоритм хорошо реализуется в аппаратуре декодера [12]. На рис. 3 представлены результаты моделирования эффективности декодирования LDPC кодов WPAN-стандарта в канале с АБГШ для случая двоичной фазовой модуляции.

При моделировании декодера использовалась арифметика с фиксированной запятой. Для представления мягких решений (LLR значений) демодулятора и сообщений внутри декодера использовался прямой код с числом разрядов $b = 8$.

Литература

1. R. G. Gallager, Low-Density Parity-Check Codes, MIT Press, Cambridge, MA, 1963. - 90 p.
2. D.J.C. MacKay and R.M. Neal. Near Shannon limit performance of low density parity check codes. Electron. Lett., Aug. 1996, vol.32, no.18. - pp.1645-1646.
3. Р. Морелос-Сарагоса. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. Перевод с английского В.Б. Афанасьева. М.: Техносфера, 2005. - 319 с.
4. Z. Li, L. Chen, L. Zeng, S. Lin, and W.-H. Fong. Efficient Encoding of Quasi-Cyclic Low-Density Parity-Check Codes. IEEE Trans. Commun., Jan. 2005, vol. 54, no. 1. - pp. 71-81.
5. IEEE P802.15.3c/July 2007, Wireless Personal Area Network (WPAN) Standard Physical Layer (PHY) specifications (Draft).
6. S. Lin and D.J. Costello Jr., Error Control Coding: Fundamentals and Applications, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2004. - 1260 p.
7. S. Lin, Quasi-Cyclic LDPC Code. CCSDS working group white paper, Oct. 2003.

8. D. Hocevar. A Reduced Complexity Decoder Architecture via Layered Decoding of LDPC Codes. In IEEE Workshop on Signal Processing System, SISP 2004, pp. 107-112.

9. M. Mansour and N.R. Shanbhad. High-throughput LDPC decoders. IEEE Trans. VLSI Syst., Dec. 2003, vol. 11, no. 6. - pp. 976-996.

10. T. Brack, M. Alles, T. Lehning-Enden, F. Kienle, N. Wehn, N.E. L'Insalata, F. Rossi, M. Rovini, L. Fanucci. Low Complexity LDPC Code Decoders for Next Generation Standards. Design, Automation & Test in Europe Conference & Exhibition, 2007. DATE '07.

11. Кравченко А.Н. Снижение сложности декодирования низкоплотного кода. «Цифровая обработка сигналов». 2010, № 2, С.35-41.

12. Кравченко А.Н. Методы и аппаратура кодирования и декодирования систематического нерегулярного кода повторения - накопления (IRA) для DVB-S2 и DVB-T2 демодуляторов. «Цифровая обработка сигналов». 2009, № 4, С.41-47.

METHODS AND APPARATUS FOR ENCODING AND DECODING QUASI-CYCLIC LOW DENSITY PARITY-CHECK CODES

Kravchenko A.N.

The analysis of the parity check matrices of irregular quasi-cyclic low-density codes (QC-LDPC) of WPAN (IEEE 802.15.3c) standard is performed. It is established that the parity check matrices are quadratic and invertible. In this connection, for the calculation of generator matrices can be used the traditional method with application to quasi-cyclic low-density codes.

The encoding and decoding methods are proposed based on the parity check matrices. The apparatus of a hardware encoding of these codes are suggested. Result of performance simulation of the decoder for QC-LDPC codes of WPAN standard over AWGN channel is presented.