ОБРАБОТКА И ПЕРЕДАЧА ИНФОРМАЦИИ

УДК 681.325.3

Н. В. Пацей, кандидат технических наук, доцент (БГТУ)

МОДЕЛИРОВАНИЕ ПЕРЕМЕННЫХ КОДОВ НИЗКОЙ ПЛОТНОСТИ ПРОВЕРОК НА ЧЕТНОСТЬ

В статье рассмотрен новый вид переменных кодов низкой плотности проверок на четность (НППЧ). Преимущество кодов заключается в особенности построения проверочной матрицы с заданными параметрами скорости кода и длины блока. Метод позволяет использовать один базовый код и различные схемы преобразования проверочной матрицы для получения широкого спектра кодов. Представлено программное средство моделирования системы кодирования-декодирования на основе предложенных переменных НППЧ кодов. В заключении приведены результаты анализа рабочих характеристик и производительности, доказывающие эффективность предложенного метода.

A new type of variable low density parity check (LDPC) code is presented in the article. The advantages of these codes are features of construction parity check matrixes with given characteristic of code rate and code length. This allows implementing a single base code that is good across a wide range of codes. Different transformation check matrix schemes is proposed to ensure code rates spectrum. The software modeling of encoding-decoding system on the base of proposed variable LDPC codes is described. Finally, simulation analysis of result codes characteristics, performance and equalizability, that prove the effectiveness of proposed approach, are done.

Введение. Качество каналов коммуникационных систем беспроводной связи в значительной степени зависит от внешних условий и в большинстве случаев является нестабильным. Для сохранения устойчивого соединения и адаптации к условиям канала в гибридной процедуре повторного запроса (HARQ – Hybrid Automatic Repeat Request) могут использоваться корректирующие коды с переменной скоростью кодирования.

Для решения данной задачи оптимальным классом помехоустойчивых кодов будут коды низкой плотности проверок на четность (НППЧ или Low Density Parity Check – LDPC) [1–3], которые имеют минимальное расстояние, линейно растущее с длиной блока, а также исправляют все ошибки вплоть до минимального расстояния при линейной сложности вероятностного итерационного алгоритма декодирования [2].

Анализ методов построения алгебраических НППЧ кодов с переменным размером блока и скоростью кода [3–5] показал, что существенными недостатками данных разработок являются небольшой диапазон скоростей кода (1/2, 2/3, 3/4, 5/6) и количество возможных перестановочных матриц, а также способов их расширения, что в конечном итоге ограничивает область их использования.

Целью настоящей работы является разработка метода конструирования проверочных матриц НППЧ кода с заданными параметрами скорости, структуры и размера базовой матрицы, величины весов строки и столбца проверочной матрицы и длины информационного блока. На основе предложенного метода необходимо было разработать компьютерную имитационную модель кодека и изучить влияние вероятности ошибки в канале связи и формата проверочной матрицы на корректирующую способность, скорость конструирования кода, а также скорость прямого и обратного преобразований.

Модель. В основе разработанной модели лежат четыре последовательных режима работы: режим генерации проверочной матрицы кода (конструирование), режим кодирования, режим передачи и режим декодирования.

Введем обозначения для входных параметров модели, которые будут определять структуру и размер проверочной матрицы кода H. Пусть k – длина информационного блока, m – размер элементарной матрицы базового кода, N – длина кодового слова, $R = k / N$ – битовая скорость кода, wr – величина веса строк проверочной матрицы H кода, а wc – величина веса столбцов проверочной матрицы (в общем случае, если wr опущена, следует считать ее равной wc).

Структурно проверочная матрица кода H состоит из двух подматриц:

$$H = [Hd|Hp], \quad (1)$$

где Hp – двойная диагональная матрица размером $(N - k) \times (N - k)$, содержащая проверочную часть (соответствует избыточным символам кодового слова) вида

$$Hp = \begin{bmatrix} I_d & - & \dots & - \\ - & I_d & \dots & - \\ \dots & \dots & \dots & - \\ - & - & \dots & I_d \end{bmatrix}, \quad (2)$$

где I_d – двойная диагональная матрица:

$$I_d = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad (3)$$

а Hd – матрица размером $(N - k) \times k$, содержащая информационную часть.

Следующий этап метода – формирование по заданному значению m квадратной матрицы базового кода P_0. В построенной модели в качестве P_0 устанавливается единичная матрица. После определения матрицы базового кода строятся перестановочные матрицы на основе операции циклического сдвига строк (или столбцов) вправо (или влево). Операция повторяется $(m - 1)$ раз, что позволяет получить $P_1, \dots, P_{m-1}$ перестановочных матриц, которые будут использоваться в дальнейшем для матрицы Hd. Возможен случай, когда перестановочные матрицы P будут частично входить в Hd. Однако в данной модели матрицы P включаются полностью.

Способ размещения перестановочных матриц Hd основан на известном алгоритме [6]. Изначально выбираются два числа a и b, принадлежащие ненулевым элементам поля Галуа $GF(m)$, где m – простое число (соответствует размеру матрицы базового кода). Заполнение матрицы Hd состоит в расстановке матриц P и нулевых квадратных матриц.

В общем случае (s, l)-элемент матрицы Hd равен:

$$P_{s,l} = b^{(s-1)} a^{(l-1)} \bmod m \quad (4)$$

для $1 \le s \le e$ и $1 \le t \le h$.

Тогда матрица Hd содержит:

$$Hd_{(N'-k',k')} = \begin{bmatrix} P_1 & P_a & P_{a^2} & \dots & P_{a^{h-1}} \\ P_b & P_{ab} & P_{a^2 b} & \dots & P_{a^{h-1}b} \\ \dots & \dots & \dots & \dots & \dots \\ P_{b^{e-1}} & P_{ba^{e-1}} & P_{a^2 b^{e-1}} & \dots & P_{a^{h-1}b^{e-1}} \end{bmatrix}. \quad (5)$$

В случае $m = wc$ в матрице Hd отсутствуют квадратные нулевые матрицы. Если $wc < m$, то необходимо расставить $(m - wc)$ нулевых матриц в каждый столбец и строку матрицы Hd. Согласно (5), количество перестановочных матриц P в столбце и строке будет соответственно:

$$e = \left[(N - k)/m\right], \quad (6)$$

$$h = \left[k/m\right]. \quad (7)$$

В полученной проверочной матрице H длина самого короткого цикла будет равна 8 и не потребуется схемы удаления циклов [6].

Однако возможен случай, когда по (6) и/или (7) будут получены наиближайшие целые e и h. Тогда для приведения размера $N' \times (N' - k')$ сконструированной проверочной матрицы H' к требуемому размеру $N \times (N - k)$, а следовательно, и скорости НППЧ кода к заданному на входе модели R будет запущена схема преобразования матрицы.

Модель содержит следующие основные схемы преобразования проверочной матрицы H':

1) схема укорочения основана на объединении двух или более строк (число строк матрицы H уменьшается, соответственно, N' остается без изменений $(N = N')$, но сокращается при этом количество проверочных разрядов $N - k'$) (рис. 1);

2) схема расширения – противоположная по сути укорочению, заключается в делении строки на две и более строк (приводит к увеличению числа проверочных разрядов и уменьшению скорости кода);

3) схема выкалывания основана на удалении строк или столбцов;

4) комбинированная схема представляет собой сочетание трех предыдущих схем.

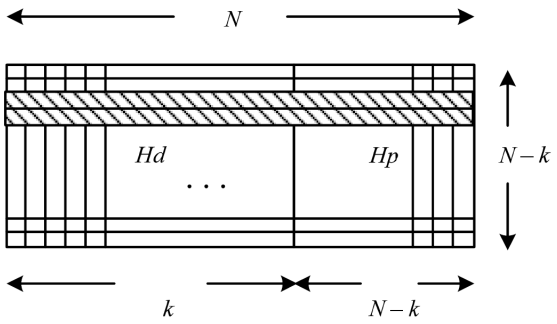

Рис. 1. Графическая интерпретация схемы укорочения проверочной матрицы H

Для выбора номеров строк и/или столбцов, участвующих в схеме преобразования, используется псевдослучайный генератор.

Применение схемы преобразования потенциально может привести к появлению циклов в проверочной матрице. Как правило, циклы длины 6 и более не оказывают существенного

влияния на качество декодирования, поэтому необходимо удалить лишь циклы длины 4. Следующий этап режима конструирования – запуск процедуры вычисления попарного скалярного произведения всех строк матрицы H. Если результат больше 1, то циклы длины 4 существуют и запускается процедура удаления коротких циклов на основе метода [7].

Таким образом, применение схем преобразования в режиме конструирования позволяет свободно управлять скоростью кода, обеспечивая практически любое значение R = 1/2, 2/3, 3/4, 3/5, 4/5, 5/6, 3/7, 4/7, 5/7, 6/7 и т. д. А метод конструирования проверочной матрицы, основанный на задании параметров k, m, R, wr, wc, дает возможность получить широкий спектр кодов с различной корректирующей способностью.

Полученная проверочная матрица H кода НППЧ является ортогональной кодовому слову, генерируемому порождающей матрицей G. Следовательно, для НППЧ кода можно получить кодовое слово напрямую из H, без использования G [2].

В режиме кодирования на основе входного информационного вектора v и сконструированной по (1) матрице H получаем кодовый вектор c:

$$c = Hv. \qquad (8)$$

Для моделирования сигнала в режиме передачи использовалась двоичная фазовая модуляция (BPSK). Блок модуляции на основе полученного по (8) вектора c формирует радиосигнал, к которому добавляется мешающее воздействие – аддитивный белый гауссовский шум (АБГШ). АБГШ характеризуется равномерной спектральной плотностью, нормально распределенным значением амплитуды, аддитивным способом воздействия на сигнал и является наиболее распространенным видом шума, используемым для расчета и моделирования систем связи. Модель позволяет изменять параметры амплитуды сигнала и мощности шума (dbW). Далее блок демодулятора выполняет перенос радиосигнала в основную полосу частот и различение передаваемых канальных символов. В режиме передачи осуществляется расчет отношения энергии сигнала, приходящейся на один бит, к уровню спектральной плотности мощности АБГШ (SNR).

Режим декодирования основан на вероятностном методе с распространением доверия [8]. Это «мягкое» декодирование выполняется на основе вектора, состоящего из вещественных величин, которые получены на выходе канала путем пересчета вероятностей. Сложность данного вида декодирования обусловлена выполнением операций с действительными числами и необходимостью вычисления апостериорных статистик для кодовых символов. Тем не менее увеличение трудоемкости окупается потенциальным улучшением эффективности режима декодирования.

Пусть $V'(i)$ – множество символов принятого вектора, которые входят в i-ю проверку: $V'(i) = \{j : Hi, j = 1\}$. Будем называть множеством $P'(j)$ – множество проверок, в которых участвует j-й символ принятого вектора: $P'(j) = \{i : Hi, j = 1\}$.

На основе принятого вектора c' формируются два (для двоичного случая) вектора вероятностей того, что в принятом векторе на данной позиции находится заданный символ:

$$f^0 = (f_0^0, \ ..., f_{V'-1}^0), f_i^0 = P(c'_i = 0) \qquad (9)$$

и

$$f^1 = (f_0^1, \ ..., f_{V'-1}^1), f_i^1 = P(c'_i = 1), \qquad (10)$$

где c'_i – элементы принятого вектора. Каждому ненулевому элементу проверочной матрицы H приписываются две величины: $q_{i,j}^x$ и $r_{i,j}^x$. Величина $q_{i,j}^x$ является вероятностью того, что j-й символ принятого вектора имеет значение x, полученное из всех проверок, кроме i-й. Величина $r_{i,j}^x$ является вероятностью того, что проверка i выполняется, если j-й символ принятого вектора равен x, а все остальные символы проверок имеют распределение вероятностей, заданное величинами $\{q_{i,j}^x : j \in V'(i) \setminus j\}$.

На первом шаге работы алгоритма требуется инициализация: значения $q_{i,j}^0$ и $q_{i,j}^1$ принимаются равными f_i^0 и f_i^1 соответственно. Для канала с гауссовским шумом инициализация производится на основе информации о дисперсии шума в канале. Для других распределений или при неизвестных характеристиках шума точная инициализация алгоритма может являться сложной задачей.

Далее алгоритм работает по принципу пересчета вероятностей символов принятого вектора, используя для перерасчета вероятностей правило Байеса для апостериорной вероятности события. Одна итерация алгоритма представляет собой следующую последовательность действий.

Для всех проверок вычисляются величины:

$$\Delta r_{i,j} = \prod_{j' \in V'(i) \setminus j} (q_{i,j'}^0 - q_{i,j'}^1) \qquad (11)$$

и пересчитываются вероятности:

$$r_{i,j}^x = \frac{1 + (-1)^x \Delta r_{i,j}}{2} \qquad (12)$$

для $x = \{0, 1\}$.

Для всех символов принятого вектора пересчитываются вероятности:

$$q_{i,j}^{x} = \alpha_{i,j} f_j^{x} \prod_{j' \in V'(i) \setminus j} r_{i,j'}^{x} \qquad (13)$$

для $x = \{0, 1\}$, где $\alpha_{i,j}$ – нормирующие коэффициенты, обеспечивающие равенство $q_{i,j}^{0} + q_{i,j}^{1} = 1$.

Формируются векторы псевдоапостериорной вероятности q_j^0 и q_j^1 следующим образом:

$$q_j^{x} = \alpha_j f_j^{x} \prod_{i \in P'(j) \setminus i} r_{i,j}^{x} \qquad (14),$$

для $x = \{0, 1\}$, где α_j – нормирующие коэффициенты, обеспечивающие равенство $q_j^0 + q_j^1 = 1$.

Формируется вектор решения c'' по следующему правилу:

$$c_j'' = \begin{cases} 1, & q_0^1 > \dfrac{1}{2}, \\ 0, & q_0^1 \le \dfrac{1}{2}. \end{cases} \qquad (15)$$

Если вектор c'' является кодовым словом, декодирование заканчивается, в противном случае выполняется следующая итерация алгоритма. В данной модели количество итераций и передаваемых блоков настраивается пользователем.

Компьютерная модель кодека была построена на языке C# с использованием принципов объектно-ориентированного программирования [9].

Результаты моделирования и их обсуждение. В ходе экспериментального моделирования (на платформе Intel Pentium T2330/1.60GHz/1.0GB) рассматривались зависимости времени конструирования проверочной матрицы (времени конструирования кода), времени кодирования и времени декодирования от длины кодового слова N (10–3200) при сохранении постоянной скорости кода R = 1/2 и 100 итерациях режима декодирования. Полученные результаты представлены в таблице.

Распределение времени преобразований НППЧ кода

N	$t_{конс}$, мс	$t_{код}$, мс	$t_{декод}$, мс
10	5	0	1
20	6	0	4,5
50	7	0	20,6
100	10	0	64,8
200	22	0	202,2
400	66	1	769,2
800	248	5,3	3 015,8
1 600	938	44,9	11 902,2
3 200	3 743	117,7	48 436,6

Анализируя данные из таблицы, можно отметить, что зависимости для всех t соответствуют квадратичному закону распределения. Важно, что время конструирования переменного НППЧ кода для заданного значения N имеет незначительный разброс значений (рис. 2). Максимальное стандартное отклонение составляет не более 40. Незначительные колебания связаны с тем, что, несмотря на структурированный метод, лежащий в основе режима конструирования, может быть использована схема преобразования проверочной матрицы H и процедура удаления коротких циклов, заложенная в модель [9]. Все это в конечном итоге вносит фактор случайности в процесс конструирования НППЧ кода. Этим и объясняется разброс величины $t_{конс}$ на рис. 2.

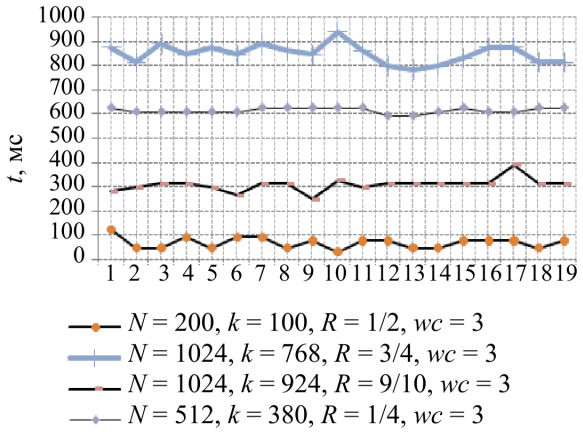

Рис. 2. Выборка времени конструирования $t_{конс}$ переменных НППЧ кодов

Сравнительный анализ (на основе таблицы) времени кодирования $t_{код}$ и декодирования $t_{декод}$ подтверждает известные результаты [8]. Так, $t_{декод}$ превышает $t_{код}$ в 50–400 раз (при 100 итерациях декодирования) и увеличивается с ростом числа итераций и длины блока.

Для изучения производительности кодов при высоких и низких отношениях сигнал/шум (0,1–10) в ходе эксперимента были промоделированы НППЧ коды с длинами кодового блока N = 200, 512, 1024, 11 224 при битовой скорости кода R = 1/4, 1/2, 3/4, 6/7, 9/10 и постоянной степени разреженности проверочной матрицы wc = 3. Как видно из рис. 3, вероятность битовых ошибок BER (Bit Error Rate) достаточно стабильна и составляет порядка 10^{-4}–10^{-5} для низких значений отношения сигнал/шум (Eb/No). BER уменьшается каждый раз на порядок с удвоением длины кодового блока (даже при уменьшении количества проверочных разрядов) и не значительно изменяется с увеличением скорости кода.

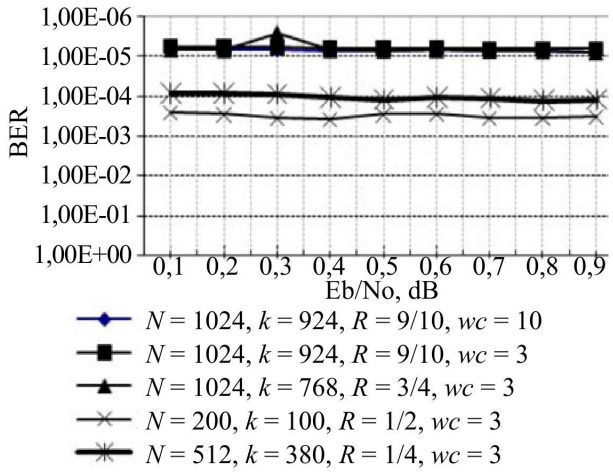

Рис. 3. Зависимость BER от низких Eb/No

Для предложенной конструкции переменного НППЧ кода при более высоких значениях Eb/No (5–10 dB) количество битовых ошибок и, соответственно, BER уменьшаются на 1–2 порядка (рис. 4).

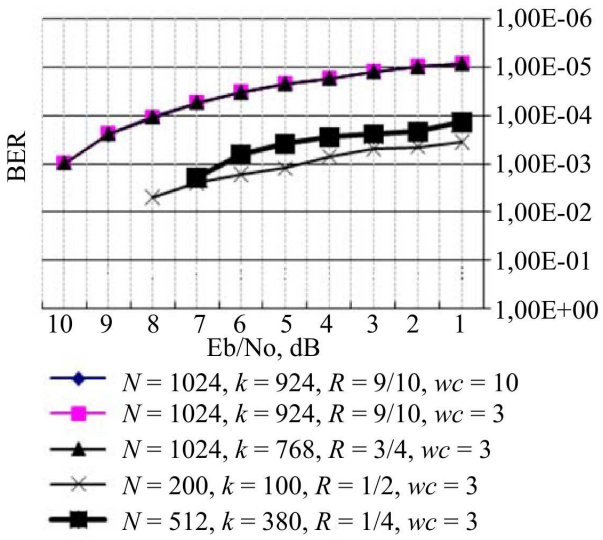

Рис. 4. Зависимость BER от высоких Eb/No

При проведении ряда экспериментов был обнаружен факт значительного разброса времени декодирования для кодов с одинаковыми входными параметрами. На рис. 5 приведены статистические данные для трех переменных НППЧ кодов (1024, 768, 3), (1024, 924, 3), (512, 380, 3).

Как видно, стандартное отклонение для представленных выборок составляет порядка 560–950. В особенности этот эффект проявляется на высоких скоростях и коротких длинах блока. Такой разброс объясняется тем, что в построенной модели был использован псевдослучайный метод выбора строк и столбцов в схеме преобразования проверочной матрицы H. Это приводит к возможной перфорации важных (с точки зрения алгоритма декодирования) проверочных бит. Следовательно, снижается вероятность и увеличивается время декодирования (рис. 5).

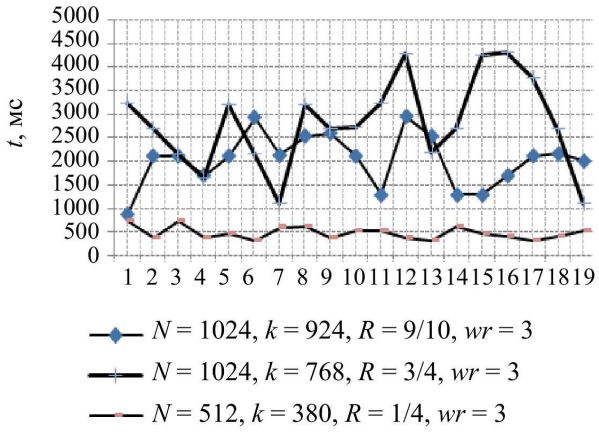

Рис. 5. Выборка времени декодирования для переменных НППЧ кодов

Заключение. На основе предложенного в статье метода конструирования переменного НППЧ кода построена имитационная компьютерная модель. В ходе моделирования исследованы временные и вероятностные характеристики полученных кодов, доказывающие эффективность предложенного метода, в особенности для больших длин блоков (>1024). Переменные НППЧ коды дают стабильно низкую вероятность ошибки BER при малых значениях отношения сигнал/шум (0,1–0,8 dB) по сравнению с известными [4, 5], а также значительно их превосходят с точки зрения диапазона скоростей.

Проблема нестабильности скорости конструирования кода $t_{конс}$ и скорости декодирования $t_{декод}$, которая в наихудшем случае для $t_{декод}$ может увеличиваться до 4 раз по сравнению со средним значением, решается на основе алгоритмического подхода.

Полученные результаты демонстрируют возможность практического использования разработанной конструкции построения переменных НППЧ кодов для систем канального кодирования.

Литература

1. RFC 5170 on Low Density Parity Check (LDPC) Staircase and Triangle Forward Error Correction (FEC) Schemes / V. Roca, C. Neumann, D. Furodet [Electronic resource]. – Mode of access: http://search.usa.gov. – Date of access: 25.06.2008.

2. Gallager, R. G. Low Density Parity Check Codes / R. G. Gallager. – Cambridge, MA: MIT. – Press, 1963. – 90 p.

3. Richardson, T. J. The capacity of low&density parity-checkcodes under message-passing decoding / T. J. Richardson, R. L. Urbanke // IEEE transactions on information theory. – 2001. – Vol. 47. – P. 10–19.

4. Kou, Y. Low Density Parity Check Codes based on Finite Geometries: A Rediscovery / Y. Kou, S. Lin, R. Fossorier // IEEE Trans. Inform. Theory. – 2001. – Vol. 47. – P. 2711–2736.

5. LDPC block and convolutional codes based on circulant matrices / R. M. Tanner [et al.] // IEEE Trans. on Inform. Theory. – 2004. – Vol. 50, № 12. – P. 2966–2984.

6. Косолапов, Ю. В. О применении схемы Озарова – Вайнера для защиты информации в беспроводных многоканальных системах передачи данных / Ю. В. Косолапов // Информационное противодействие угрозам терроризма: науч.-практ. журн. – 2007. – № 10. – С. 111–120.

7. Improved low-dencity parity-check codes using irregular graphs and brelief propogation / M. G. Luby [et al.] // Proc. of IEEE Intern. Symposium on Inform. Theory. – Cambridge. Mass., 1998. – P. 171.

8. Свидетельство о регистрации компьютерной программы ECC v.2.0 / М. М. Кебич, Н. В. Пацей, Д. М. Романенко, Д. В. Шиман; заявитель Белорус. гос. технол. ун-т. – № 260; заявл. 16.12.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010.

Поступила 02.03.2011