УДК 621.391

СИНТЕЗ НИЗКОПЛОТНОСТНЫХ КОДОВ НА ОСНОВЕ УРАВНОВЕШЕННЫХ НЕПОЛНЫХ БЛОК-СХЕМ

Овинников А.А., *научный сотрудник кафедры телекоммуникаций и основ радиотехники Рязанского государственного радиотехнического университета, e-mail: ovinnikovalexey@gmail.com*

Рассматривается задача построения эффективных с точки зрения энергетического выигрыша декодирования алгебраических кодовых конструкций низкоплотностных кодов для высокоскоростных систем передачи информации с малой избыточностью. Её решение основано на теории комбинаторики и смежных подразделов. Эффективность полученных кодов оценивается с помощью имитационного моделирования по методу Монте Карло, а также путём вычисления ряда принципиальных параметров, присущих LDPC кодам.

Ключевые слова: помехоустойчивое кодирование, итеративное декодирование, низкоплотностные коды, уравновешенные неполные блок-схемы, системы Штейнера.

Введение

В настоящее время особое значение приобретают задачи повышения надёжности и достоверности передаваемой информации. Эффективным средством решения такой задачи является использование теории и практики помехоустойчивого кодирования.

На сегодняшний день существует огромное множество различных методов и алгоритмов канального кодирования и декодирования, которые отличаются друг от друга по сложности реализации, энергетическому выигрышу, а также другим показателям. Однако, доминирующее положение с позиции энергетической эффективности, широты внедрения, а также перспективы дальнейшего развития теории и практики помехоустойчивого кодирования занимают итеративно-декодируемые конструкции, к которым относятся турбо и низкоплотностные (LDPC) коды. Среди этих двух ансамблей LDPC коды, впервые рассмотренные Р. Галлагером [1], обладают эффективным алгоритмом декодирования, сложность которого с ростом длины кодового слова (N) пропорциональна O(N). Кроме того, они могут применяться для исправления как одиночных, так и пакетных ошибок без необходимости применения процедуры перемежения, что существенно сказывается на задержке, присутствующей при обработке информации.

Существенной проблемой теории низкоплотностных кодов является отсутствие достаточного количества алгоритмов синтеза, позволяющих получать коды в большом диапазоне кодовых длин и скоростей, обладающих алгебраически стройной структурой, которая с лёгкостью может быть перенесена на современную элементную базу.

В данной работе рассматривается задача построения эффективных с точки зрения энергетического выигрыша декодирования алгебраических кодовых конструкций для высокоскоростных систем передачи информации с малой избыточностью. Её решение основано на теории комбинаторики и смежных подразделах. Эффективность полученных кодов оценивается с помощью имитационного моделирования по методу Монте Карло, а также путём вычисления ряда принципиальных параметров, присущих LDPC кодам.

Классификация кодов, полученных на основе УНБС

Конструктивные методы построения LDPC кодов [2] всегда привязаны к некоторым строго определённым математическим объектам. В частности, в настоящей работе рассматриваются коды, синтезированные на основе так называемых уравновешенных неполных блок-схем (УНБС, BIBD – balance incomplete block design) [3]. Уравновешенной неполной блок-схемой называется такое размещение υ различных элементов по b блокам, что каждый блок содержит ровно k различных элементов, каждый элемент появляется точно в r различных блоках и каждая пара различных элементов a_i и a_j появляется точно в λ блоках. Таким образом, любая УНБС может быть задана вектором из пяти связанных друг с другом чисел – $(\upsilon, b, r, k, \lambda)$, которые в свою очередь имеют между собой детерминированную связь вида:

$$\begin{aligned} &b \cdot k = \upsilon \cdot r; \\ &r(k-1) = \lambda(\upsilon - 1). \end{aligned} \qquad (1)$$

Существование зависимостей (1) позволяет использовать сокращённый способ записи УНБС с тремя независимыми параметрами: (υ, k, λ), где υ – количество элементов, k – число блоков в УНБС и λ – количество поэлементных сочетаний между блоками. Графически любую блок-схему можно представить в виде набора блоков или матрицей инцидентности, в частности, для υ=b=7, r=k=3, λ=1 существует единственная УНБС вида:

$$\begin{aligned} &B_0 = (0,1,3); \\ &B_1 = (1,2,4); \\ &B_2 = (2,3,5); \\ &B_3 = (3,4,6); \\ &B_4 = (4,5,0); \\ &B_5 = (5,6,1); \\ &B_6 = (6,0,2); \end{aligned} \qquad A = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

где $A = (a_{ij})$, $i = 1,\ldots,\upsilon$, $j = 1,\ldots,b$; причём $a_{ij} = \begin{cases} 1, & \text{если } a_i \in B_j, \\ 0, & \text{если } a_i \in B_j \end{cases}$, где a_{ij} и B_j – элементы и блоки УНБС соответственно. Если внимательно присмот-

реться к предлагаемому примеру, то не трудно обнаружить, что укороченная на 3 последних строки матрица инцидентности А представляет собой не что иное, как проверочную матрицу самого короткого кода Хэмминга. Аналогичным образом на основе выбранной математической абстракции для больших значений параметров (υ, k, λ) можно получать и другие классы канальных кодов, в том числе и низкоплотностные с проверочной матрицей (H). Любая матрица инцидентности соответствующая блок-схеме с параметрами (υ, k, λ) обладает следующими свойствами:

– любая строка или столбец содержит r и k ненулевых элементов соответственно;

– любая пара строк или столбцов имеет максимум λ общих ненулевых позиций.

Исходя из свойств УНБС, гарантировать отсутствие циклов длины 4 в графах Таннера LDPC [2] кодов возможно лишь при λ=1. Таким образом, появляется первое существенное ограничение, накладываемое на УНБС, которое приводит к сужению множества блок-схем до подмножества так называемых систем Штейнера (υ, k, 1) [3]. Среди всех систем Штейнера особый интерес представляет подмножество циклических блок-схем с различным количество элементов υ=(3,4,5,…). В целом используемую в работе классификацию УНБС можно изобразить в форме вложенных подмножеств, представленных на рис. 1. Цифрами отмечено количество элементов υ в каждой из блок-схем подмножества.

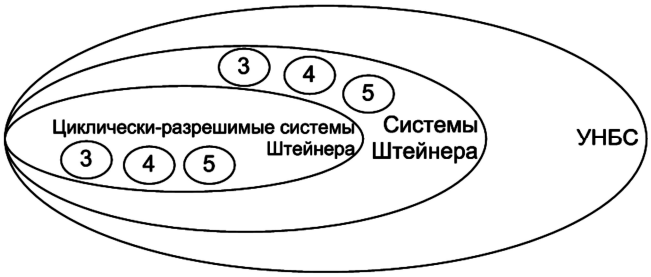
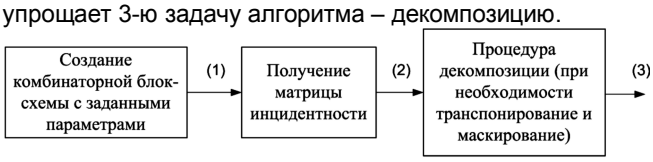


Рис. 1. Представление УНБС в виде вложенных множеств

Обобщённый алгоритм синтеза LDPC кодов

Учитывая свойства блок-схем, а также структуру рассмотренных выше матриц инцидентности, не трудно сформулировать обобщённый алгоритм синтеза LDPC кодов на базе используемых в данной работе математических абстракций. Процедура получения проверочной матрицы низкоплотностного кода на базе УНБС изображена в форме последовательного набора операций, представленных блоками на рис. 2. Первый и последний блок в представленном алгоритме являются наиболее трудоёмкими и вариативными. На первом этапе выполнения процедуры (рис. 2.) ставится задача получить УНБС с заданными параметрами. При этом могут использоваться различные комбинаторные объекты и структуры [3].

Стоит отметить, что далеко не все возможные блок-схемы подходят для синтеза LDPC кодов. К выбору параметров следует подходить с особой тщательностью. Рассматриваемая на рис. 2. процедура формирования кодов обладает достаточно большой вариативностью, которая позволяет создавать проверочные матрицы H (4) в широком диапазоне кодовых длин и скоростей. При этом для одного и того же набора параметров (υ, k, λ) может быть получено множество различных LDPC кодов. Алгоритм создания УНБС может существенно отличаться в зависимости от выбора величины λ, однако, чаще всего её принимают равной единице, что существенно упрощает 3-ю задачу алгоритма – декомпозицию.



(1) – УНБС (υ, k, λ), (2) – A, (3) - H

Рис. 2. Обобщённый алгоритм синтеза LDPC кодов на основе комбинаторных блок-схем

Системы Штейнера, как математическая основа построения LDPC кодов, и их свойства

Рассмотрим общие свойства, присущие ансамблю LDPC кодов, которые получены из систем Штейнера. Известно [3], что матрицы инцидентности этого математического множества имеют максимально возможное число блоков b для всех УНБС. Это приводит к тому, что LDPC код, сформированный на базе такой системы, обладает максимально возможной скоростью среди всех кодов с обхватом графа Таннера g_0=6, весом столбца d_s=k и числом проверочных уравнений M=b. Ранг проверочной матрицы H может оказаться неполным, что дополнительно увеличивает кодовую скорость, которая ограничена снизу величиной [4]:

$$R \geq 1 - \frac{k(k-1)}{\upsilon - 1}. \qquad (2)$$

Кроме того, число независимых строк в матрице инцидентности систем Штейнера характеризуется следующей нижней границей [4]:

$$Rank_2(H) \geq (k-1)\sqrt{(r-1)r/k}, \qquad (3)$$

тогда кодовая скорость ограничена сверху, как:

$$R \leq 1 - \frac{k(k-1)\sqrt{(\upsilon-1)(\upsilon-k)/k}}{\upsilon(\upsilon-1)}, \qquad (4)$$

Графически зависимость кодовой длины от скорости для реально существующих квазициклических кодов на основе систем Штейнера представлена на рис. 3. Параметр k для каждой УНБС варьируется от 3-х до 5-ти, однако может быть и большим. Нетрудно заметить, что скорость кодирования крайне быстро стремится к 1 с ростом длины кода.

Важным подклассом систем Штейнера являются так называемые циклически-разрешимые системы, для которых характерно то, что общее количество блоков b можно разделить на r подгрупп (дубликатов) таким образом, что исключение одной из них уменьшает величину r для всех υ элементов одинаково. В силу того, что асимптотический анализ ансамблей регулярных LDPC кодов [5] показывает, что для всех скоростей кодирования наибольшим энергетическим выигрышем в ОСШ в канале с белым шумом показывают коды с d_s=3 далее будет предложен обобщённый алгоритм их формирования на основе соответствующих систем Штейнера.

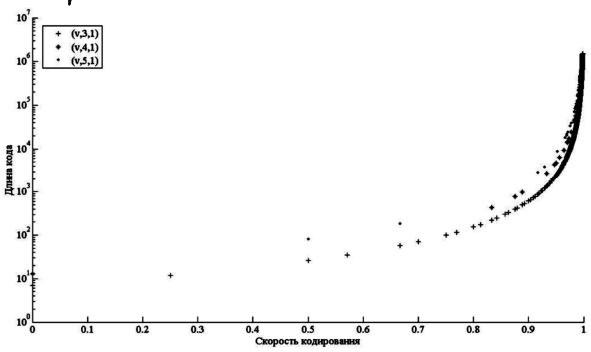


Рис. 3. Зависимость кодовой длины от скорости для LDPC кодов построенных на базе различных систем Штейнера

Блок-схема с k=3 и λ=1 вполне естественно называется системой троек Штейнера. Параметры этой УНБС удовлетворяют следующим равенствам, полученным из (1):

$$b = \frac{\upsilon(\upsilon-1)}{6}, \quad r = (\upsilon-1)/2. \qquad (5)$$

Необходимым и достаточным условием существования троек Штейнера является выполнение тождества вида

$$\upsilon \equiv 1, \quad 3 (\mathrm{mod}\, 6). \qquad (6)$$

Таким образом [3], если $\upsilon = 6t+1$ или $\upsilon = 6t+3$, при целом значении числа t, существует система троек Штейнера порядка υ. Некоторые УНБС рассматриваемого подмножества представлены в табл. 1 и 2. Разделение троек Штейнера на 2 группы не случайно, т.к. алгоритмы их получения в том случае, когда базовые блоки b формируют циклические группы, оказываются различными.

Обобщённый алгоритм синтеза LDPC кодов на основе систем Штейнера

Задача формирования подмножества циклических и одновременно разрешимых троек Штейнера оказывается далеко не тривиальной. Однако в работах [6] было показано, что на основе различных комбинаторных последовательностей можно сформировать абсолютно все тройки из ансамбля (υ, 3, 1). Принимая во внимание этот факт, можно предложить обобщённый алгоритм формирования проверочных матриц LDPC кодов на базе описанных выше блок-схем (рис. 4). Фактически алгоритм позволяет по заданным параметрам подсистемы канального кодирования (K, N) получить проверочную матрицу H регулярного низкоплотностного кода с квазициклической структурой. Предлагаемая на рис. 4. процедура состоит из 3-х этапов, первый из которых заключается в получении некоторых комбинаторных последовательностей и их модификаций, получивших своё название в честь авторов – T. Skolem и A. Rosa [6]. Длина получаемой последовательности S аналитически связана с входными параметрами кодирования следующим образом:

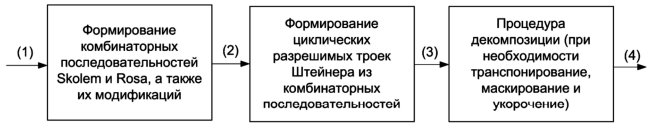
$$n=(K-1)/6, \qquad (7.1)$$

$$n=(K-3)/6, \qquad (7.2)$$

$$n = \max\left(\frac{K-3}{6}-1,\ \frac{K-1}{6}+1\right), \qquad (7.3)$$

причём конкретное значение величины n определяется вычислением каждого из представленных выражений, с приоритетом выбора от 7.1 к 7.3. Главное условие, чтобы n являлось целым числом. Таким образом, в случае если первое и второе выражения дадут дробные значения, искомая величина размерности комбинаторной последовательности будет найдена по формуле (7.3), как максимальное целое значение в диапазоне указанном в скобках. На втором этапе алгоритма набор чисел S будет использован для синтеза циклически разрешимых троек Штейнера с помощью известных в математике [3, 6] процедур.

В итоге получается система Штейнера с известной матрицей инцидентности, результатом декомпозиции которой является искомый LDPC код. Может получиться такая ситуация, когда параметры кода, полученного на выходе обобщённого алгоритма синтеза (рис. 4, (1)), не совпадают с входными. В этом случае в 3-ем блоке схемы предусмотрена процедура укорочения проверочной матрицы H.



(1) – параметры кода LDPC (K,N)
(2) - комбинаторная последовательность S
(3) - циклическая разрешимая тройка Штейнера (v, 3, 1)
(4) - проверочная квазициклическая матрица LDPC кода

Рис. 4. Обобщённый алгоритм синтеза проверочных матриц LDPC кодов на базе циклических разрешимых троек Штейнера

Результаты имитационного моделирования LDPC кодов

Оценим энергетическую эффективность помехоустойчивых LDPC кодов, полученных с помощью обобщённого алгоритма, представленного на рис. 4. В силу того, что кодовая скорость R для выбранного ансамбля быстро стремится к единице с ростом параметра N (рис. 3), выбрать походящие для сравнения конструкции Таннера не представляется возможным. Поэтому в качестве конкурирующих решений были взяты наиболее распространённые алгоритмы синтеза псевдослучайных кодов (Mac, PEG) [7, 8]. Каждый из них способен генерировать проверочные матрицы произвольной длины и скорости, регулярной и нерегулярной структуры с заданными весовыми функциями $\lambda(x)$ и $\rho(x)$. Отличия между выбранными алгоритмами кроются лишь в том, что второй – PEG, максимизирует локальный обхват графа Таннера, а первый – Mac, пытается как можно точнее воспроизвести заданное весовое распределение с учётом g_0=6. Процедура оценки помехоустойчивости кодов выполнялась по методу Монте Карло в канале с аддитивным белым гауссовским шумом и двоичной фазовой модуляцией. Декодирование осуществлялось по алгоритму BP [7], причём максимальное количество итераций фиксировалось значениями 10 и 50. Целесообразность такого ограничения заключается в необходимости оценить возможный дополнительный энергетический выигрыш декодера при кратном увеличении вычислительных затрат. Кроме того, для оценки потенциальной близости выбранных конструкций к пределу Шеннона [9] каждой кодовой длине и скорости было поставлено в соответствие минимальное значение отношения сигнал-шум (σ_{min}), для которого возможен безошибочный приём. Для численного моделирования были выбраны шесть различных кодов, параметры которых представлены в табл. 3.

Имитационное моделирование выполнялось с шагом равным 0.5 дБ, причём для получения достоверной точки необходимо было накопить более 1000 ошибок на каждом шаге ОСШ. Результаты эксперимента представлены зависимостями вероятности ошибки на бит (p_b) от отношения сигнал-шум (E_b/N_0) на рис. 5-10. Разница в энергетической эффективности оценивается по уровню p_b=10^{-6}. Для каждого кода при заданном числе итераций декодирования вычислено значение превышения предельного уровня ОСШ σ_{min} выраженное в децибелах и отражено в табл. 4 (ΔS).

Кроме того, для каждой пары кодов найдены значения относительных энергетических выигрышей $\Delta a(i)$–$a(j)$=$E_b/N_0(a(i))$ – $E_b/N_0(a(j))$ для 10 и 50 итераций декодирования, где $a(i)$ и $a(j)$ – наименование соответствующего алгоритма синтеза низкоплотностного кода. Параметр ΔS-$a(i)$= σmin – $E_b/N_0(a(i))$ показывает на сколько энергетическая эффективность выбранного кода отличается от предельно возможной.

Таблица 1. Первые десять троек Штейнера порядка $\upsilon = 6t + 1$

t	1	2	3	4	5	6	7	8	9	10
υ	7	13	19	25	31	37	43	49	55	61
r	2	4	6	8	10	12	14	16	18	20
b	7	26	57	100	155	222	301	392	495	610

Таблица 2. Первые десять троек Штейнера порядка $\upsilon = 6t + 3$

t	1	2	3	4	5	6	7	8	9	10
υ	9	15	21	27	33	39	45	51	57	63
r	4	7	10	13	16	19	22	25	28	31
b	12	35	70	117	176	247	330	425	532	651

Таблица 3. Параметры LDPC кодов, используемых в имитационном моделировании

№	R	M	N	σ_{min}
1	2/3	19	57	1,059
2	0,7	21	70	1,275
3	0,833	37	222	2,361
4	0,842	39	247	2,457
5	0,9	61	610	3,199
6	0,903	63	651	3,247

Таблица 4. Результаты имитационного моделирования LDPC кодов

M	$\Delta_{Mac\text{-}PEG}$ 10/50 ит., дБ	$\Delta_{Mac\text{-}STS}$ 10/50 ит., дБ	$\Delta_{PEG\text{-}STS}$ 10/50 ит., дБ	Δ_{S_Mac}, дБ	Δ_{S_PEG}, дБ	Δ_{S_STS}, дБ
19	2,41/2,09	2,51/2,14	0,1/0,05	7,581	5,541	5,491
21	2,62/2,21	2,56/2,01	-0,06/-0,2	7,355	5,125	5,325
37	2/1,45	2/1,52	0/0,07	4,899	3,449	3,379
39	1,39/1	1,47/1,05	0,08/0,05	4,353	3,353	3,303
61	1,13/0,7	1,18/0,75	0,05/0,05	3,211	2,511	2,461
63	0,88/0,67	0,99/0,7	0,11/0,03	3,153	2,483	2,453

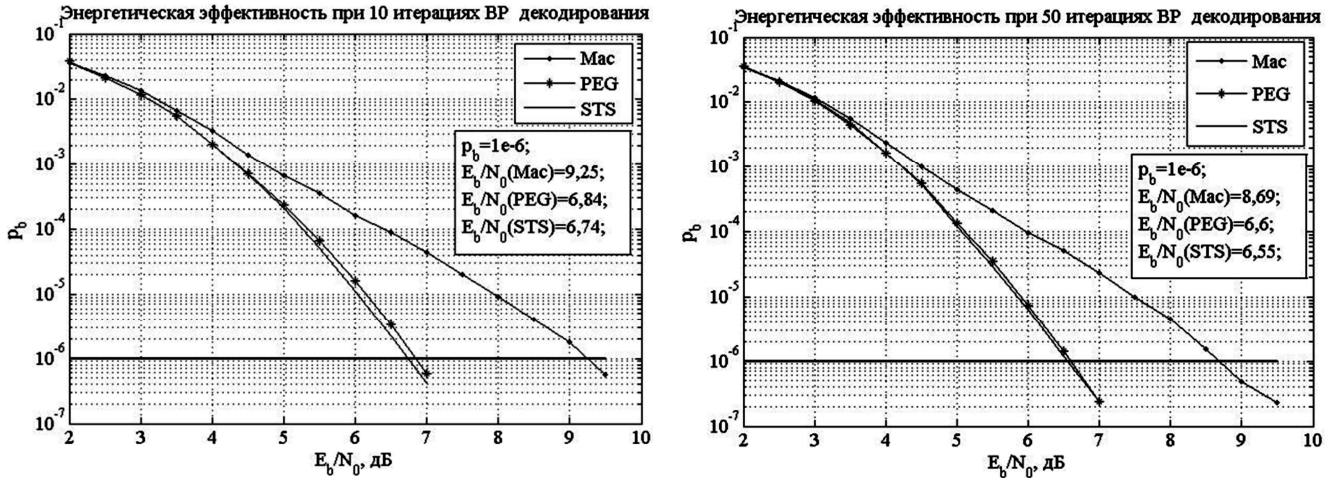


Рис. 5. Энергетическая эффективность низкоплотностных кодов с параметрами M=19, N=57 при различном числе итераций декодирования

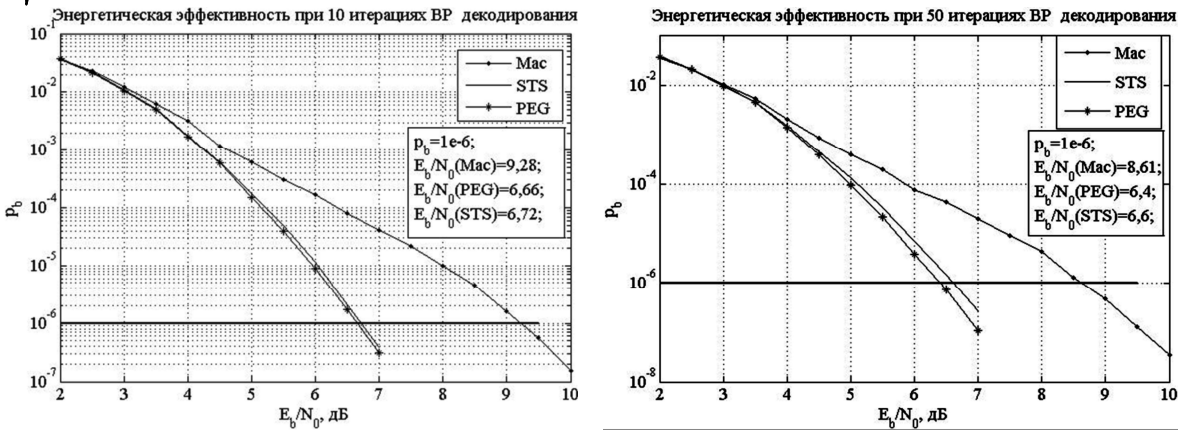


Рис. 6. Энергетическая эффективность низкоплотностных кодов с параметрами M=21, N=70 при различном числе итераций декодирования

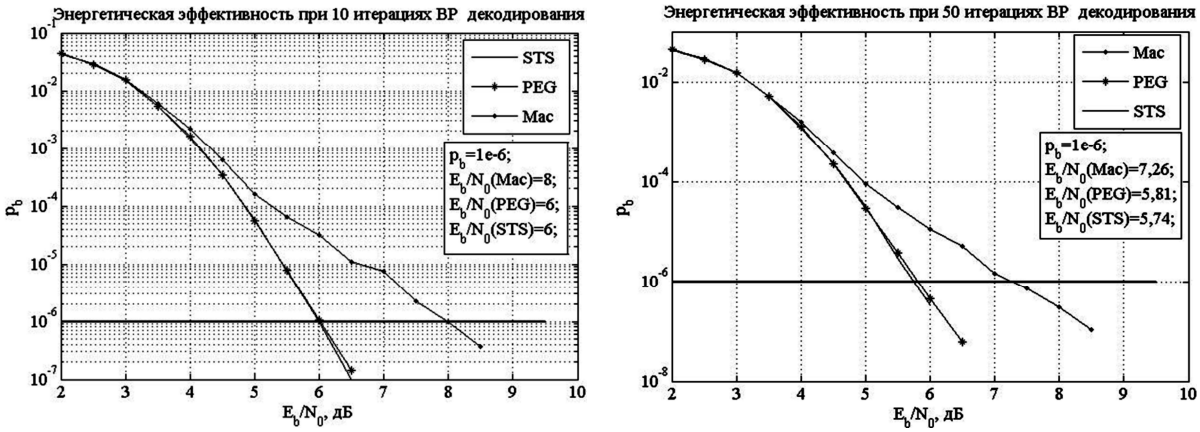


Рис. 7. Энергетическая эффективность низкоплотностных кодов с параметрами M=37, N=222 при различном числе итераций декодирования

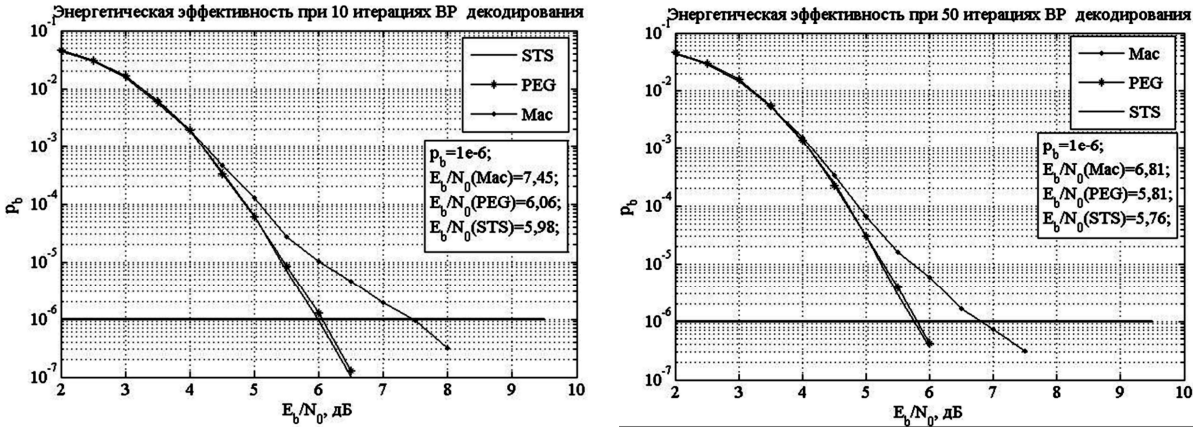


Рис. 8. Энергетическая эффективность низкоплотностных кодов с параметрами M=39, N=247 при различном числе итераций декодирования

Таким образом, судя по результатам, представленным на рис. 5-10, а также в табл. 4, коды, синтезированные на основе комбинаторных последовательностей, показывают значительно лучшие результаты по сравнению с псевдослучайными кодами Маккая (Mac). Численное значение выигрыша в ОСШ для предлагаемых конструкций варьируется в диапазоне от 0,7 до 2,56 дБ и зависит исключительно от длины кода и числа итераций декодирования. Такое преимущество получено не случайно, а связано с тем, что для высоких скоростей кодирования, а также малых длин N<100 рассматриваемые псевдослучайные алгоритмы синтеза не могут создать граф Таннера, не имеющий циклов минимальной длины, следовательно, g_0=4. Это, в свою очередь, приводит к значительной деградации помехоустойчивости и делает неоспоримым преимущество предлагаемых квазициклических LDPC кодов по сравнению с Mac конструкцией. Однако, при сравнении с кодами PEG, преимущество в энергетической эффективности оказывается не столь очевидным, варьируется в пределах 0,03-0,1 дБ, и в одном эксперименте (рис. 6) даже наблюдается незначительный проигрыш, до 0,2 дБ. Но даже при столь малой разнице в помехоустойчивости синтезированный по обобщённому алгоритму ансамбль LDPC кодов обладает одним неоспоримым преимуществом – квазициклической структурой, которая крайне удобна при реализации подсистемы кодирования на аппаратном уровне.

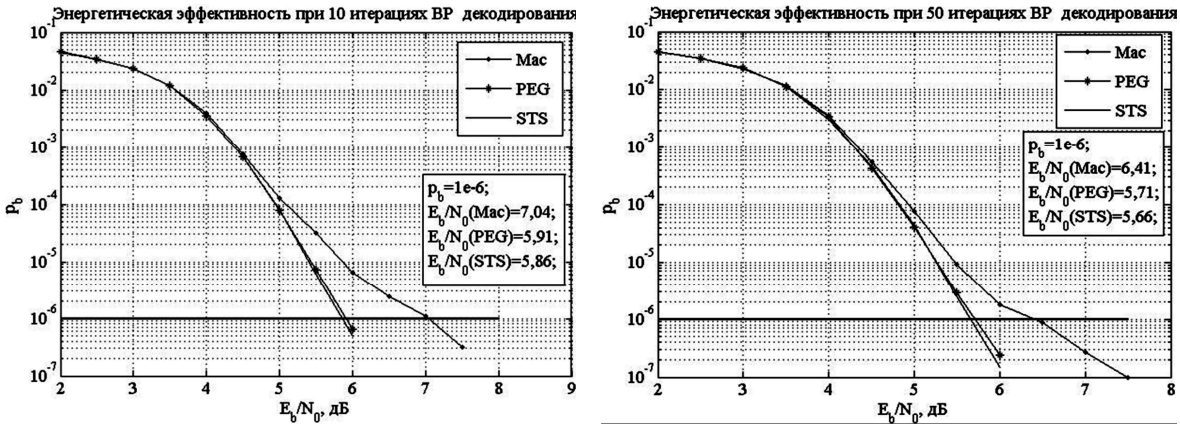


Рис. 9. Энергетическая эффективность низкоплотностных кодов с параметрами M=61, N=610 при различном числе итераций декодирования

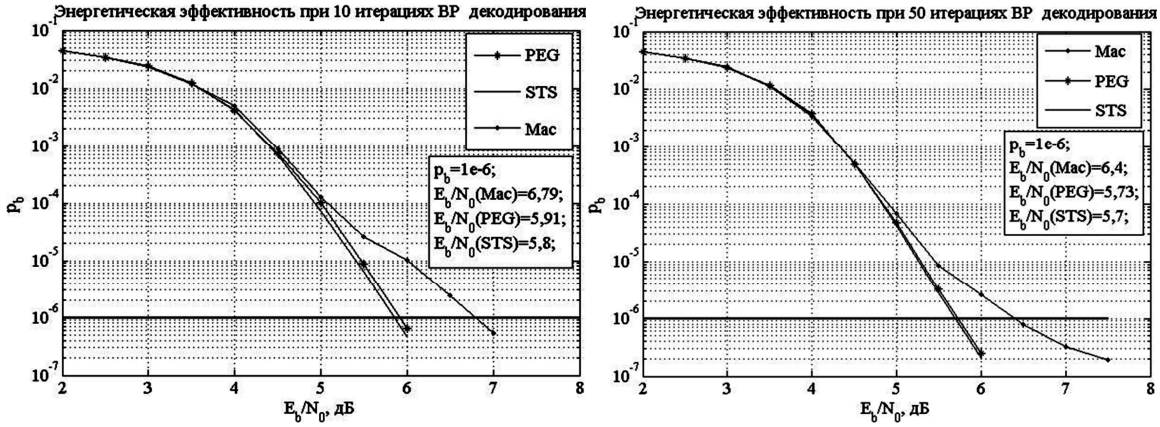


Рис. 10. Энергетическая эффективность низкоплотностных кодов с параметрами M=63, N=651 при различном числе итераций декодирования

Заключение

В работе проведено имитационное моделирование низкоплотностных кодов, синтезированных на основе уравновешенных неполных блок схем, которые в свою очередь базируются на комбинаторных последовательностях Сколема и Роса. Сформированные коды показали хорошие результаты по помехоустойчивости в сравнении с подклассом псевдослучайных кодов (Mac); полученный энергетический выигрыш декодирования лежит в диапазоне от 0,7 до 2,56 дБ. Обобщённый алгоритм синтеза (рис. 4), предлагаемый в данной работе, позволяет получать ансамбли квазициклических LDPC кодов с различными кодовыми длинами и скоростями, что потенциально расширяет границы применения подобных конструкций. Одним из направлений дальнейших исследований является поиск наиболее эффективных кодов в рамках синтезированного ансамбля.

Исследование выполнено за счет гранта Российского научного фонда (проект 14-19-01263) в Рязанском государственном радиотехническом университете.

Литература

1. Gallager R.G. Low-Density Parity-Check Codes. Cambridge MA:MIT Press, 1963.

2. Ryan W.E. and Lin S. «Channel Codes. Classical and Modern», Cambridge University Press, 2009.

3. Холл М. Комбинаторика, Издательство «МИР», М. 1970.

4. Johnson S.J. and Weller S.R. Regular low-density parity-check codes from combinatorial designs. In Proc. IEEE Information Theory Workshop (ITW2002), p. 90-92, Cairns, Australia, September 2001.

5. Richardson T.J., Shokrollahi M.A, and Urbanke R.L. Design of capacity approaching irregular low-density parity-check codes. IEEE Trans. Inform. Theory, 47(2):619–637, February 2001.

6. Colbourn C.J. and Rosa A. Triple Systems. Oxford University Press, 1999.

7. MacKay D.J.C. Good error-correcting codes based on very sparse matrices. IEEE Trans. Inform. Theory, 45(2):399–431, March 1999.

8. Arnold D.M., Eleftheriou E., and Hu X.Y., «Progressive edgegrowth Tanner graphs», in Proc. IEEE Global Telecommun. Conf., San Antonio, TX, Nov. 2001, vol. 2, pp. 995–1001.

9. Shannon C.E. A mathematical theory of communication. Bell Sys. Tech. J.,27:379–423, 623–656, July–Oct. 1948.

BALANCE INCOMPLETE BLOCK DESIGNS BASED LDPC CODES

Ovinnikov A.A.

In this paper the problem of constructing efficient algebraic Low-Density Parity Check codes for high data transmission with low redundancy is considered. Code design algorithm is based on the theory of combinatorics and related subsections. The effectiveness of codes, which are used in the reseach, is evaluated using Monte Carlo simulations, as well as by calculating the number of fundamental parameters inherent to LDPC codes.