

Федеральное государственное бюджетное учреждение науки
ИНСТИТУТ ПРОБЛЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ
им А. А. Харкевича Российской академии наук

На правах рукописи

Кондрашов Константин Александрович

**Разработка конструкций сверточных кодов с
малой плотностью проверок**

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2013

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институте проблем передачи информации им. А. А. Харкевича Российской академии наук (ИППИ РАН).

Научный руководитель:

доктор технических наук,

Зяблов Виктор Васильевич

Официальные оппоненты:

Зигангиров Камиль Шамильевич,

доктор технических наук, старший научный сотрудник, ИППИ РАН, главный научный сотрудник лаборатории №1

Владимиров Сергей Михайлович,

кандидат физико-математических наук, инженер программист в ООО “Одноклассники”

Ведущая организация:

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Защита состоится «30» октября 2013 г. в 15.00 часов на заседании диссертационного совета Д 212.156.04 при Московском физико-техническом институте (ГУ) по адресу: 141700, г. Долгопрудный, Московская обл., Институтский пер., д. 9, ауд. 204 Нового корпуса.

С диссертацией можно ознакомиться в библиотеке МФТИ (ГУ).

Автореферат разослан «28» сентября 2013 г.

Ученый секретарь

диссертационного совета Д 212.156.04

кандидат физико-математических наук

Стрыгин Леонид Васильевич

Общая характеристика работы

Актуальность работы. Объемы накапливаемой и обрабатываемой в современном мире информации непрерывно возрастают, повышаются и требования к скорости и достоверности передачи данных по каналам связи. Для достижения меньших вероятностей ошибок при передаче, согласно фундаментальным результатам теории кодирования, необходимо использовать все более длинные коды. Однако, при выборе длинных кодов недостаточно руководствоваться только их корректирующими свойствами. Определяющими факторами применимости таких кодов, наряду с хорошими асимптотически корректирующими свойствами, становятся сложность кодирования и декодирования. Возникает задача построения и исследования эффективных кодов, имеющих реализуемые с помощью современных технических средств алгоритмы кодирования и декодирования. Реализуемыми принято считать алгоритмы кодирования и декодирования с неэкспоненциальной сложностью. Наиболее известными и широкоупотребимыми кодами этого класса являются коды с малой плотностью проверок (МПП). МПП коды были предложены Р. Г. Галлагером в 1962 г. В работах В. В. Зяблова и М. С. Пинксеры 1974 г. и 1975 г. было показано, что минимальное расстояние МПП кодов растет линейно с длиной кода и были предложены просто реализуемые алгоритмы декодирования. Однако, несмотря на хорошие потенциальные корректирующие свойства, МПП коды долгое время игнорировались.

В настоящее время МПП кодам посвящается множество работ. Реализуемые корректирующие свойства МПП кодов при неэкспоненциальной сложности декодирования исследовались в работах К. Ш. Зигангирова и Д. К. Зигангирова 2006 г., а также в работе К. Ш. Зигангирова, А. Е. Пусане, Д. К. Зигангирова и Д. Дж. Костелло 2008 г. При итеративном декодировании МПП коды обеспечивают лучший обмен в отношении помехоустойчивость к сложности декодирования. В работе Хименеса и Зигангирова 1999 г концепция МПП кодов Галлагера была применена к сверточным кодам. Далее, в работе А. Е. Пусане, Д. К. Зигангирова и Д. Дж. Костелло были исследованы границы минимального и свободного расстояний и было доказано, что пороги МПП сверточных кодов приближаются к пропускным способностям каналов.

Таким образом, исследование свойств различных конструкций сверточных МПП кодов представляет особый теоретический интерес. При этом как теоретическое, так и практическое значение имеет исследование как потенциальных, так и реализуемых при декодировании с неэкспоненциальной сложностью корректирующих свойств.

Цель диссертационной работы состоит в разработке конструкций сверточных кодов с малой плотностью проверок, алгоритмов декодирования с неэкспоненциальной сложностью, применимых к кодам предложенных кон-

струкций, теоретическом и практическом исследовании их корректирующих свойств.

Научная новизна состоит в следующем:

- Разработан класс сверточных кодов с единичной памятью и малой плотностью проверок (ЕП МПП). Получены теоретические оценки свободного и активных расстояний. Показано, что при скоростях $R \leq 0.5$ граница свободного расстояния ЕП МПП кодов совпадает с границей Томмесена–Юстесена свободного расстояния случайных ЕП кодов.
- Разработан итеративный алгоритм декодирования ЕП МПП кодов с малой сложностью. Написаны программы моделирования. Методом имитационного моделирования проведено исследование влияния выбора параметров ЕП МПП кодов на реализуемые корректирующие свойства.
- Разработан класс 4-плетеных сверточных кодов (4-П-СМПП) с малой плотностью проверок. Экспериментально установлены метрические свойства.
- Разработаны итеративные алгоритмы декодирования 4-П-СМПП кодов с малой сложностью. Написаны программы моделирования. Методом имитационного моделирования проведено исследование реализуемых корректирующих свойств.

Практическая значимость. Работа носит теоретический характер. Предложенные конструкции сверточных МПП кодов с относительно небольшими кодовыми блоками в кодовых последовательностях позволяют при терминировании получать блоковые коды, не уступающие по потенциальным и реализуемым корректирующим свойствам более длинным блоковым МПП кодам, выигрывая при этом в сложности кодирования и декодирования и дополнительных возможностях кодеров и декодеров. Результаты, изложенные в диссертации, могут быть использованы при разработке новых систем связи и стандартов передачи данных.

На защиту выносятся следующие положения:

- предложена конструкция сверточных кодов с единичной памятью, построенных на основе блоковых кодов с малой плотностью проверок (ЕП МПП), и рассмотрены потенциальные корректирующие свойства;
- предложен ансамбль ЕП МПП кодов, получены асимптотические характеристики лучших кодов в ансамбле;

- предложена конструкция сверточных кодов с малой плотностью проверок, получаемых плетением четырех кодов компонентов с одним проверочным уравнением (4-П-СМПП), проведены расчеты дистанционных характеристик;
- разработаны и исследованы алгоритмы декодирования для кодов предложенных конструкций, написаны программные реализации алгоритмов, проведено имитационное моделирование.

Апробация работы. Основные результаты диссертации докладывались на следующих конференциях: IEEE International Symposium on Information Theory (2011), International Workshop on Algebraic and Combinatorial Coding Theory (2010, 2012), XII Symposium on Problems of redundancy in information and control systems (2009), конференциях молодых ученых и специалистов ИППИ РАН “Информационные технологии и системы” (2009, 2010, 2011). Результаты работы используются на практике, в частности, при выполнении НИР «Методы обеспечения качества обслуживания при доступе к широкополосным мультимедийным услугам в беспроводных самоорганизующихся сетях», проводимой ИППИ РАН по Соглашению №8330 (2012 г.) с Министерством образования и науки России.

Публикации. Материалы диссертации опубликованы в 6 печатных работах, из них 3 статьи в рецензируемых журналах [1, 2, 6], 3 статьи в сборниках конференций [3–5].

Личный вклад автора. Все основные научные положения и выводы, составляющие содержание диссертации, разработаны автором самостоятельно. Теоретические и практические исследования, а также вытекающие из них выводы и рекомендации проведены и получены автором лично. Подготовка к публикации полученных результатов проводилась совместно с соавторами. Все теоретические результаты работ [1–4], [5] получены автором самостоятельно. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Подготовка к публикации полученных результатов проводилась совместно с соавторами.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения и библиографии. Общий объем диссертации 95 страниц, включая 31 рисунок. Библиография включает 45 наименований на 6 страницах.

Содержание работы

Во Введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана

(Ч) ЕП МПП-кодов, $K + \nu < N$, $\nu \leq K$ удовлетворяют следующим условиям:

$$\begin{aligned}\hat{d}_1^r &\geq \min(d(C_c), d(C_0) + d(C_p)), \\ \hat{d}_2^r &\geq d(C_0) + \min(d(C_{pc}), d(C_{pcf}) + d(C_p)), \\ \hat{d}_j^r &\geq \hat{d}_2^r + (j - 2)d(C_{pcf}),\end{aligned}$$

где $d(C_i)$ – минимальный вес кода C_i .

Кодовые расстояния $d(C_i)$ МПП кодов, выраженных через порождающие матрицы, неизвестны. Дальнейший анализ выполняется через проверочные матрицы.

Для получения асимптотической оценки используются методы, применяемые в случае блочных МПП кодов. В соответствии с леммой 1, в кодовой последовательности из $j + 1$ (или j в случае неполной памяти) блоков никакие из двух соседних кодовых подблоков не являются нулевыми, поэтому для оценки кодового расстояния можно исследовать участок проверочной матрицы \mathbf{H}_{put} ,

$$\begin{bmatrix} \mathbf{H}_p & & & & \\ \mathbf{H}_c & & & & \\ \mathbf{H}_f & \mathbf{H}_p & & & \\ & \mathbf{H}_c & & & \\ & \mathbf{H}_f & & & \end{bmatrix}$$

как проверочную матрицу блочного кода МПП. Перепишем проверочную матрицу блочного кода в общем виде:

\mathbf{H}_1		
\mathbf{H}_2		\mathbf{H}_3
		\mathbf{H}_4

Обозначим коды с проверочной матрицей такого вида, где подблоки выбираются из ансамблей $\mathcal{E}(n_0, \ell_i, b)$, $i = 1, \dots, 4$, $\ell_1 = \ell_4$, $\ell_2 = \ell_3$, МПП кодов Галлагера, ансамблем \mathcal{E}_{ch} . Асимптотическую оценку кодового расстояния по ансамблю \mathcal{E}_{ch} можно получить методом Галлагера.

Пусть $N_{ch}(W)$ – среднее число кодовых слов веса W в ансамбле \mathcal{E}_{ch} . В ансамбле найдется хотя бы один код с минимальным расстоянием $d_{ch} > W_0$, если $\sum_{W=2}^{W_0} N_{ch}(W) < 1$. Сформулируем следующую теорему:

Т е о р е м а 1. Если существует положительный корень δ_0 уравнения

$$\frac{\ell_2}{n_0} \log \left(\frac{(1 - \frac{\delta}{2-\delta})^{2n_0} + (1 + \frac{\delta}{2-\delta})^{2n_0}}{2} \right) - \delta \ell \log \left(\frac{\delta}{2-\delta} \right) + \frac{\ell_1 + \ell_4}{n_0} \log \left(g_0 \left(\frac{\delta}{2-\delta} \right) \right) - 2H \left(\frac{\delta}{2} \right) (\ell - 1) = 0$$

относительно переменной δ , то в ансамбле $\mathcal{E}_{ch}(\ell_1, \ell_2, n_0, b)$ существуют коды с относительным расстоянием больше δ_0 .

Доказательство. Выразим среднее число кодовых слов заданного веса в ансамбле \mathcal{E}_{ch} через вероятность $P(W)$ случайного слова $\mathbf{r} = (\mathbf{r}_{12} \mathbf{r}_{34})$ веса W оказаться кодовым в ансамбле:

$$N_{ch}(W) = \binom{2n}{W} P(W).$$

Пусть $N_i(W)$ – среднее число кодовых слов веса W в ансамбле МПП-кодов $\mathcal{E}(n_0, \ell_i, b)$, а $P_i(\mathbf{S}_j|x)$ – вероятность получить для слова веса x синдром \mathbf{S}_j в ансамбле кодов $\mathcal{E}(n_0, \ell_i, b)$. Среднее число кодовых пар с заданными весами W_{12} и W_{34} в ансамблях $\mathcal{E}(n_0, \ell_1, b)$ и $\mathcal{E}(n_0, \ell_4, b)$ оценивается произведением $N_1(W_{12})N_4(W_{34})$. Вероятность в зависимости от веса получить совпадающие синдромы для ансамблей $\mathcal{E}(n_0, \ell_2, b)$ и $\mathcal{E}(n_0, \ell_3, b)$ можно описать суммой по всем возможным синдромам:

$$\sum_{\mathbf{S}_j} P_2(\mathbf{S}_j|W_{12})P_3(\mathbf{S}_j|W_{34}).$$

Таким образом, слово веса W окажется кодовым в ансамбле \mathcal{E}_{ch} с вероятностью

$$P(W) = \frac{\sum_{y=0}^W \left(N_1(y)N_4(W-y) \sum_{\mathbf{S}_j} P_2(\mathbf{S}_j|y)P_3(\mathbf{S}_j|W-y) \right)}{\binom{2n}{W}}, \quad (5)$$

Наибольшая вероятность случайного слова $\mathbf{r} = (\mathbf{r}_{12} \mathbf{r}_{34})$ веса W и длины $2n$ оказаться кодовым в ансамбле \mathcal{E}_{ch} в зависимости от распределения веса между частями \mathbf{r}_{12} и \mathbf{r}_{34} достигается при $\text{wt}(\mathbf{v}_{12}) = \text{wt}(\mathbf{v}_{34}) = W/2$.

Оценив сумму в 5 наибольшим членом и взяв значение в точке $y = \frac{W}{2}$, получим

$$\frac{2^{-b\ell_2} \left(\frac{W}{2bn_0-W} \right)^{-W\ell} \left(\left(1 - \frac{W}{2bn_0-W} \right)^{2n_0} + \left(1 + \frac{W}{2bn_0-W} \right)^{2n_0} \right)^{\ell_2 b} \left[g_0 \left(\frac{W}{2bn_0-W} \right) \right]^{(\ell_1+\ell_4)b}}{\binom{n}{W/2}^{2\ell-2}}.$$

Таким образом,

$$P(W) \leq \frac{2^{-b\ell_2} W \left(\frac{W}{2bn_0-W} \right)^{-W\ell} \left(\left(1 - \frac{W}{2bn_0-W} \right)^{2n_0} + \left(1 + \frac{W}{2bn_0-W} \right)^{2n_0} \right)^{\ell_2 b} \left[g_0 \left(\frac{W}{2bn_0-W} \right) \right]^{(\ell_1+\ell_4)b}}{\binom{2n}{W} \binom{n}{W/2}^{2\ell-2}}$$

и среднее число кодовых слов $N_{ch}(W) = \binom{2n}{W}P(W)$ веса W в ансамбле \mathcal{E}_{ch} ограничено сверху:

$$N_{ch}(W) \leq \frac{2^{-b\ell_2} W \left(\frac{W}{2bn_0 - W}\right)^{-W\ell} \left(\left(1 - \frac{W}{2bn_0 - W}\right)^{2n_0} + \left(1 + \frac{W}{2bn_0 - W}\right)^{2n_0} \right)^{\ell_2 b} \left[g_0 \left(\frac{W}{2bn_0 - W}\right) \right]^{(\ell_1 + \ell_4)b}}{\binom{n}{W/2}^{2\ell - 2}}. \quad (6)$$

До тех пор, пока $\sum_{W=2}^{W=2n} N_{ch}(W) < 1$, в ансамбле найдется хотя бы один код с минимальным расстоянием $d_{ch} > W$. Пусть δ - относительное расстояние, $\delta = \frac{W}{N}$, тогда асимптотическая оценка относительного кодового расстояния может быть получена из условия

$$\log \left(\frac{2^{-b\ell_2} (n_0 b \delta)^2 \left(\frac{\delta}{2-\delta}\right)^{-bn_0 \delta \ell} \left(\left(1 - \frac{\delta}{2-\delta}\right)^{2n_0} + \left(1 + \frac{\delta}{2-\delta}\right)^{2n_0} \right)^{\ell_2 b} \left[g_0 \left(\frac{\delta}{2-\delta}\right) \right]^{(\ell_1 + \ell_4)b}}{2^{2N b_0 H(\frac{\delta}{2}) (\ell - 1)}} \right) \leq 0.$$

$$F(\delta) = \frac{\ell_2}{n_0} \log \left(\frac{\left(1 - \frac{\delta}{2-\delta}\right)^{2n_0} + \left(1 + \frac{\delta}{2-\delta}\right)^{2n_0}}{2} \right) - \delta \ell \log \left(\frac{\delta}{2-\delta}\right) + \frac{\ell_1 + \ell_4}{n_0} \log \left(g_0\left(\frac{\delta}{2-\delta}\right)\right) - 2H\left(\frac{\delta}{2}\right) (\ell - 1).$$

▲

Асимптотическая граница свободного расстояния ЕП МПП кодов с полной памятью на скоростях до $R = 0.5$ и максимально допустимой частичной памятью при скоростях выше, следует из лемм 1–3 и теоремы 1. Граница ЕП МПП кодов представлена на рис. 1 вместе с границами Костелло и Томмеса–Юстесена для сверточных кодов и границей Варшамова–Гилберта для блочковых кодов. В случае полной памяти асимптотическая граница свободного расстояния ЕП МПП кодов совпадает с границей Томмеса–Юстесена для случайных ЕП кодов.

Во второй главе предложен итеративный алгоритм декодирования ЕП-МПП кодов, построенный на основе алгоритма декодирования “распространения доверия”. Проведено исследование корректирующих свойств ЕП-МПП кодов методом имитационного моделирования.

В § 2.1 дано общее описание алгоритма распространения доверия и его модификации на случай сверточных ЕП МПП кодов. Обозначим с помощью $\mathcal{N}(i)$ множество символьных узлов, связанных с проверочным узлом c_i , а с помощью $\mathcal{L}(n)$ множество проверочных узлов, связанных с символьным

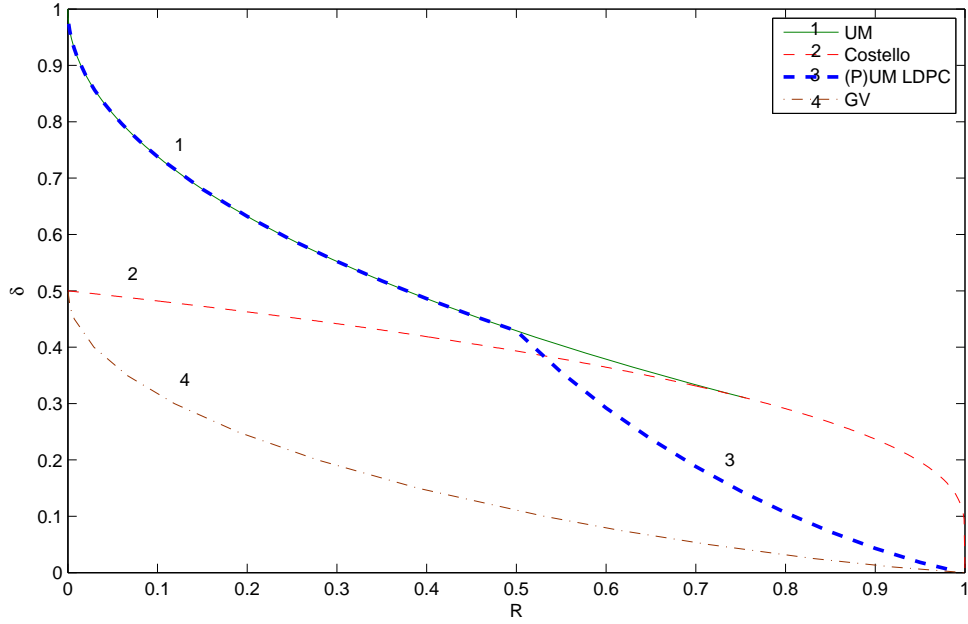


Рис. 1. Асимптотические границы относительного свободного расстояния. GV – граница Варшавова-Гилберта, Costello – граница Костелло, UM – граница Томмесена-Юстесена для кодов с полной единичной памятью, (P)UM LDPC – граница свободного расстояния для кодов с (частично)единичной памятью, полученных из блочных МПП-кодов.

узлом v_n . Пусть кодовое слово блочного (N, ℓ, n_0) МПП кода $\mathbf{v} = (v_1 v_2 \dots v_N)$ передается по АБГШ каналу и пусть $\mathbf{r} = (r_1 r_2 \dots r_N)$ означает принятую последовательность.

Алгоритм распространения доверия основан на вычислении по принятой последовательности апостериорных вероятностей

$$P(v_n = 0 | \mathbf{r}) \quad (7)$$

для кодовых символов v_n , $n = 1, 2, \dots, N$.

Операции, производимые декодером распространения доверия на j -ом шаге, $j = 1, 2, \dots, I$, могут быть разделены на две фазы. В первой фазе проверочные узлы получают сообщения от смежных с ними символьных узлов и, используя полученную информацию, формируют новое сообщение. Во второй фазе проверочные узлы посылают вновь сформированные сообщения смежным с ними символьным узлам, а те, в свою очередь, формируют новые сообщения, которые будут посланы ими на первой фазе следующего шага итеративного процесса декодирования.

Опишем i -ый, $i = 1, 2, \dots, I - 1$ шаг итеративного процесса декодирования. Во время первой фазы i -ой итерации n -ый символьный узел посылает сообщение $z_{ni}^{(i-1)}$, которое было вычислено им на предыдущем шаге, смежному проверочному узлу $i \in \mathcal{L}(n)$. Затем i -ый проверочный узел, $i = 1, 2, \dots, \ell b$,

получивший n_0 сообщений $z_{ni}^{(i-1)}$, $n \in \mathcal{N}(i)$, от смежных символьных узлов, вычисляет статистики $y_{ln}^{(i)}$, $n \in \mathcal{N}(i)$,

$$y_{ln}^{(i)} = \log \frac{1 + \prod_{n' \in \mathcal{N}(i) \setminus \{n\}} \tanh(z_{n'i}^{(i-1)}/2)}{1 - \prod_{n' \in \mathcal{N}(i) \setminus \{n\}} \tanh(z_{n'i}^{(i-1)}/2)}, \quad (8)$$

Во время второй фазы i -ого итеративного процесса декодирования, $i = 1, 2, \dots, I - 1$, i -ый проверочный узел, $i, i = 1, 2, \dots, \ell b$, посылает сообщение $y_{ln}^{(i)}$ n -ому символьному узлу, $n \in \mathcal{N}(i)$. Затем n -ый символьный узел вычисляет статистики (см. (??)),

$$\begin{aligned} z_{ni}^{(i)} &= z_n^{(0)} + \sum_{i' \in \mathcal{L}(n) \setminus \{i\}} y_{i'n}^{(i)} \\ &= z_n^{(0)} + \sum_{i' \in \mathcal{L}(n) \setminus \{i\}} \log \frac{1 + \prod_{n' \in \mathcal{N}(i') \setminus \{n\}} \tanh(z_{n'i'}^{(i-1)}/2)}{1 - \prod_{n' \in \mathcal{N}(i') \setminus \{n\}} \tanh(z_{n'i'}^{(i-1)}/2)} \end{aligned} \quad (9)$$

которые данный символьный узел будет рассылать как сообщения на следующем шаге итеративного процесса. Этим завершается вторая фаза i -го шага процесса итеративного декодирования, $i = 1, 2, \dots, I - 1$.

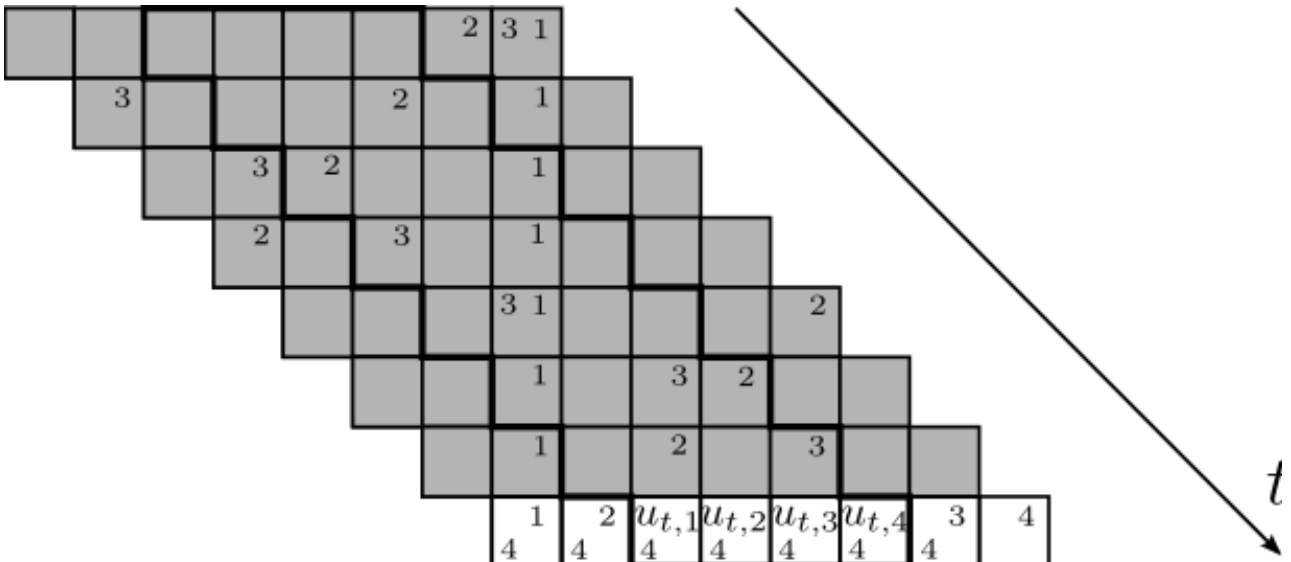
В § 2.2 рассмотрено декодирование терминированных методом нулевого хвоста последовательностей ЕП-МПП кодов. Проведено имитационное моделирование для различных выборов параметров кодов.

В § 2.3 рассмотрено декодирование терминированных методом циклического замыкания хвоста последовательностей ЕП-МПП кодов. Проведено имитационное моделирование для различных выборов параметров кодов.

В § 2.4 рассмотрено декодирование последовательностей ЕП-МПП кодов, для которых проверочные матрицы блочных МПП кодов выбирались не из общего ансамбля МПП кодов Галлагера, а из ансамбля МПП кодов, построенных на основе системы троек Штейнера. Метод построения частного случая МПП кодов выбран для устранения коротких циклов в деревьях декодируемых кодов. Проведено имитационное моделирование для различных выборов параметров кодов.

В третьей главе предлагается конструкция q -ичных 4-плетеных МПП кодов, выполняется исследование дистанционных свойств кодов предложенного ансамбля.

В § 3.1 Описана конструкция 4-плетеных сверточных МПП кодов и несколько способов их кодирования. 4-ПСМПП код получается ‘плетением’ четырех кодов-компонентов – горизонтального, вертикального, и двух – *диагональных*. 4-ПСМПП код имеет следующую структуру:



где закрашенные ячейки представляют кодовые символы, а индексами обозначена принадлежность символов к коду-компоненту.

В произвольный момент времени для получения на выходе закодированного блока v_t на первом шаге кодируются вертикальный и диагональные коды-компоненты. Затем информационный блок u_t и полученные проверочные символы кодируются горизонтальным кодом-компонентом. Конструкцию 4-плетеных сверточных кодов можно рассматривать, как развитие идеи 2-плетеных сверточных кодов К.Ш. Зигангирова.

Кодирование П-СМПП-кодов может выполняться несколькими способами. Один из алгоритмов кодирования сверточного МПП-кода следует напрямую из рекуррентного уравнения кодовой последовательности сверточных кодов. Пусть, без потери общности, символы информационного блока u_t стоят на первых b позициях кодового блока v_t . Пусть $v_t = [v'_t | v''_t]$, $v'_t = u_t$ и H_0^T состоит из первых b строк матрицы $H_0^T(t)$, а H''_0^T – из оставшихся $c - b$. Напомним, что подматрица $H_0^T(t)$, $t \in \mathbb{N}$ имеет полный ранг $c - b$. Тогда проверочные символы кодового блока v_t являются единственным решением системы линейных уравнений

$$-v''_t H''_0^T(t) = v'_t H_0^T(t) + v_{t-1} H_1^T(t) + \dots + v_{t-m_s} H_{m_s}^T(t).$$

В аппаратной реализации такого кодирования можно использовать сдвиговые регистры. Объем памяти, необходимый для хранения символов из поля, составляет $c \cdot m_s + b$ ячеек. Сложность кодирования линейна относительно длины N П-С-МПП-кода.

Второй алгоритм кодирования не хранит в памяти предыдущие блоки кодовой последовательности, вместо этого он использует дополнительную информацию, доступную после кодирования предыдущего блока. Опишем алгоритм. В любой момент времени t кодовая последовательность v удовлетворяет условию

$$v_{[0,t-1]} H_{[0,t-1]}^T = [\mathbf{0}_{[0,t-1]} | s_t], \quad (10)$$

где $s_t = [s_{t,1} s_{t,2} \dots s_{t,m_s}]$ – вектор *частичных синдромов*. На самом деле, вектор частичных синдромов s_t – это не что иное как состояние кодера σ_t в момент времени t . Вектор частичных синдромов вычисляется рекуррентно в соответствии со следующим правилом:

$$s_{t,i} = \begin{cases} s_{t-1,i+i} + v_{t-1} H_i^T(t+i-1), & i = 1, \dots, m_s - 1 \\ v_{t-1} H_{m_s}^T(t+m_s-1), & i = m_s. \end{cases} \quad (11)$$

Кодовый блок $v_t = [v'_t | v''_t]$, $v'_t = u_t$ находится из решения – $[u_t | v''_t] H_0^T(t) = s_{t,1}$.

Необходимый объем памяти в этом случае составляет $(c - b) \cdot m_s$ q -ных ячеек, что меньше, чем при первом алгоритме. При этом вычислительная сложность остается такой же. При аппаратной реализации для вычисления частичных синдромов можно использовать сдвиговый регистр.

Для построения ансамбля сверточных плетеных МПП кодов, коды представляются в виде графа Таннера, к которому затем применяется “расширение”. Для построения ансамбля П-СМПП-кодов $\mathfrak{E}(L)$, используются, выбираемые равновероятно, случайные матрицы перестановок P размера $L \times L$. Применяя к графу Таннера B операцию “копирование с перестановками”: $b_{i,j} = b_{i,j} P_{i,j}$, каждому ребру графа B ставится в соответствие матрица перестановки, все узлы графа копируются L раз, а конечные точки ребер представляются

В § 3.2 комбинаторно исследованы дистанционные свойства кода базовой конструкции. Для нахождения активных расстояний d_j для различных длин j решается система линейных уравнений $x H_{[1,j+m_s-1]}^T = \mathbf{0}$, из которой исключены первые несколько строк, отвечающих нулевым проверочным символам вертикального и диагональных кодов-компонентов в первом кодовом блоке. Система уравнений имеет единственное нулевое решение или множество решений. В последнем случае найденные линейно независимые решения системы образуют фундаментальную систему решений (ФСР), линейная оболочка которой дает все решения. Найдем среди векторов линейной оболочки ФСР ненулевой вектор с минимальным весом. Его вес дает точное значение активного расстояния d_j . Результаты вычисления активных расстояний П-СМПП-кодов представлены на рис. 2.

На рис. 2 также представлены результаты для 2-плетеных МПП кодов, в структуре которых используются только вертикальный и горизонтальный коды-компоненты. Наблюдаемые активные расстояния оказываются лучше в случае 4-плетеных МПП кодов. При практически одинаковой длине кодов-компонентов, к такому результату приводит увеличенное число слоев и большая память.

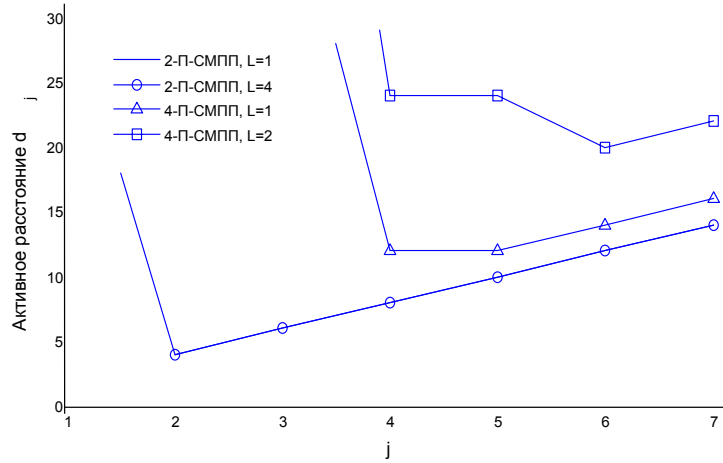


Рис. 2. Активные расстояния ПСМПП кодов

В четвертой главе предложены итеративные алгоритмы декодирования. Опишем итеративный алгоритм с жестким принятием решений \mathcal{A}_1 . Пусть \mathbf{r} – принятое из канала слово, содержащее ошибки. На произвольной итерации i , $i \in \mathbb{N}$ на вход декодера подается слово $\mathbf{r}(\mathbf{i})$, где $\mathbf{r}(0) = \mathbf{r}$, выходом декодера является слово $\mathbf{r}(\mathbf{i}+1)$. Для декодирования слов, относящихся к определенным кодам-компонентам, используются соответствующие компонентные декодеры $\{\mathcal{D}^{(k)}\}_{k=1}^J$.

Каждая итерация декодирования состоит из следующих шагов:

А л г о р и т м \mathcal{A}_1 :

1. для каждого кода-компонента с помощью декодера компонента $\mathcal{D}^{(k)}$ декодируются все соответствующие ему слова из $\mathbf{r}^{(i)}$. Результаты запоминаются в $\mathbf{r}_k^{(i)}$;
2. создается слово следующей итерации $\mathbf{r}^{(i+1)}$, символы $r_j^{(i+1)}$ которого определяются мажоритарной функцией выбора по большинству из $r_{k,j}^{(i+1)}$ (в дальнейшем будем называть эту функцию *голосованием*). Если выбор неоднозначен, то в качестве значения символа $r_j^{(i+1)}$ выбирается значение соответствующего символа $r_j^{(i)}$ из входного слова итерации;
3. вычисляется синдром слова $\mathbf{r}^{(i+1)}$.

В конце каждой итерации в зависимости от значения синдрома и номера итерации возможны четыре исхода:

1. переход к следующей итерации;
2. успех декодирования;

3. ошибка декодирования;
4. отказ от декодирования.

Переход к следующей итерации. Переход осуществляется при ненулевом синдроме выходного слова, если выходное слово итерации отличается от входного слова итерации и не достигнут предел итераций: $i < I_{\max}$, $r^{(i+1)} \neq r^{(i)}$.

Успех декодирования. Успех декодирования происходит в том случае, если синдром выходного слова нулевой и декодированное кодовое слово совпадает с переданным: $S(r^{(i+1)}) = \mathbf{0}$, $r^{(i+1)} = v$.

Ошибка декодирования. Происходит при нулевом синдроме, когда принятое слово декодировано в другое кодовое слово, не совпадающее с переданным: $S(r^{(i+1)}) = \mathbf{0}$, $r^{(i+1)} \neq v$.

Отказ от декодирования. Отказ происходит при ненулевом синдроме, если исчерпаны итерации или результирующее слово итерации не отличается от входного слова итерации: $S(r^{(i+1)}) \neq \mathbf{0}$, $r^{(i+1)} = r^{(i)} \vee i = I_{\max}$.

При декодировании П-СМПП-кодов алгоритмом \mathcal{A}_1 , если в принятом слове много ошибок, то довольно часто может происходить ситуация, когда для некоторого символа все коды-компоненты дают разные решения или имеется несколько подмножеств кодов-компонентов, давших одинаковые решения, с максимальным весом. В двоичном случае решение для символа принимается только если больше половины кодов-компонентов дали одинаковое решение. В q -ичном случае для 4-П-СМПП-кода решение происходит только если несколько кодов компонентов дали одинаковое решение, а остальные коды-компоненты дали несовпадающие друг с другом решения. На поздних итерациях, когда большинство ошибок исправлено (или внесены новые устойчивые ошибки), невозможность решения для символа приводит с большой вероятностью к отказу декодирования, так как декодируемое слово не изменяется. Возможность выйти из получившегося ‘тупика’ могла бы способствовать улучшению результатов декодирования. В качестве такой возможности мы предлагаем использовать введение внешним декодером стираний. Критерием введения стираний служит невозможность принятия решения для символа с помощью мажоритарной функции голосования.

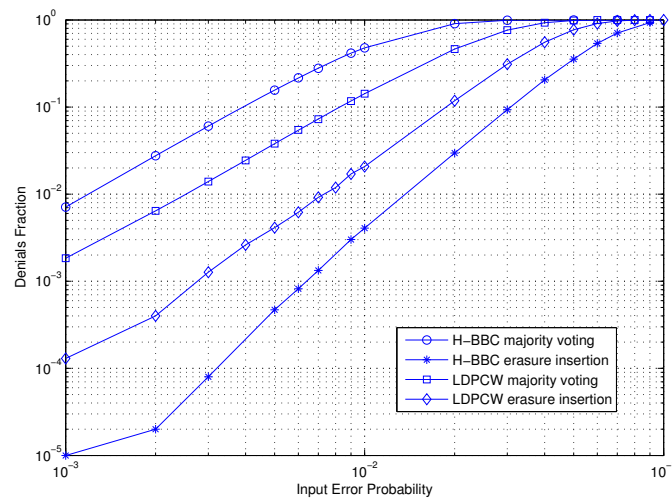
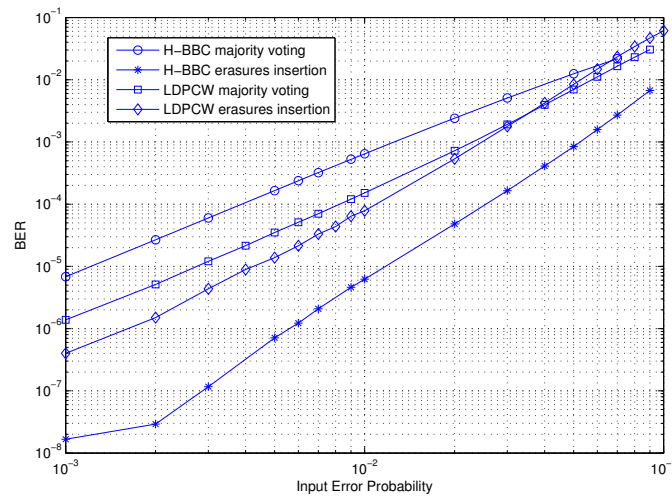
А л г о р и т м \mathcal{A}_2 :

1. для каждого символа $r_j^{(i)}$ входного слова итерации i декодеры кодов-компонентов $\mathcal{D}^{(k)}$ вычисляют соответствующие значения, удовлетворяющие проверкам кодов-компонентов. Результаты запоминаются в $\mathbf{r}_k^{(i)}$;
2. создается слово следующей итерации $\mathbf{r}^{(i+1)}$, символы $r_j^{(i+1)}$ которого

определяются голосованием по большинству из $r_{j,k}^{(i+1)}$. Если выбор не определен, то на месте символа $r_j^{(i+1)}$ вводится стирание;

3. стирания в слове $\mathbf{r}^{(i+1)}$ исправляются алгоритмом \mathcal{A}_1 с декодерами $\{\mathcal{E}^{(k)}\}_{k=1}^J$ кодов-компонентов, исправляющими стирания, до полного устранения;
4. вычисляется синдром слова $\mathbf{r}^{(i+1)}$.

В § 4.2 проведено исследование корректирующих свойств методом имитационного моделирования. Результаты представлены на рис. 3. Результаты декодирования 4-плетеных МПП кодов с q -ичными кодами-компонентами – кодами Рида–Соломона сравниваются с результатами декодирования 2-плетеных кодов, с кодами-компонентами – кодами Хэмминга (отмечены на рис. Н-ВВС) с аналогичной памятью. При более простом декодировании 4-ПСМПП коды



оказываются предпочтительнее.

В Заключении приведены основные результаты, полученные в диссертационной работе:

- предложена конструкция сверточных кодов с единичной памятью, на основе блоковых кодов с малой плотностью проверок (ЕП МПП);
- исследована структура кодовых последовательностей ЕП МПП кодов, получены аналитические оценки на характеристики кодов;
- предложен ансамбль ЕП МПП кодов, получены асимптотические характеристики лучших кодов в ансамбле. Полученная граница свободного расстояния, при скоростях $R < 0.5$, совпадает с границей Томмеса — Юстесена, полученной существенно большем классе кодов – случайных сверточных кодов с единичной памятью;
- предложен алгоритм декодирования на основе алгоритма распространения доверия, разработаны программы и проведено имитационное моделирование;
- предложена конструкция сверточных кодов, получаемых плетением 4-х кодов компонентов (4-П-СМПП), проведены расчеты для части дистанционных характеристик;
- предложены итеративные алгоритмы декодирования с линейной сложностью итерации, разработаны программы и проведено имитационное моделирование.

Список публикаций

1. Зяблов В.В, Кондрашов К.А., Скопинцев О.Д. Оценка активных расстояний сверточных кодов (частично) единичной памяти с малой плотностью проверок // Информационные процессы. 2012. Р. 372 –388.
2. Зяблов В. В, Кондрашов К.А. Конструкция плетеных сверточных кодов на базе кодов проверки на четность с одним проверочным символом // Информационно-управляющие системы. 2011. Р. 156 –159.
3. Зяблов В.В, Кондрашов К.А. Декодирование Q-ных плетеных сверточных МПП-кодов // Информационные технологии и системы (ИТиС), Геленджик, Россия. 2010. Р. 85 –88.

4. Зяблов В.В, Кондрашов К.А. Граница свободного расстояния случайных кодов с (частично) единичной памятью // Информационные технологии и системы (ИТиС), Геленджик, Россия. 2011. Р. 53 –60.
5. Kondrashov K., Zyablov V. On the lower bound of the free distance of partial unit memory codes based on LDPC Codes // ISIT. 2011. Р. 1831–1835.
6. Zyablov V. V., Kondrashov K. A., Skopintsev O. D. On the Active Distances of Partial Unit Memory Codes Based on LDPC Codes // Journal of Communications Technology and Electronics,. 2013. Р. 636–647.

Подписано в печать 23.09.2013

Заказ № 8772 тираж 100 экз.

Печать трафаретная

Типография "11-й ФОРМАТ"

ИНН 7726330900

115230, Москва, Варшавское ш., 36

(499) 788-78-56

www.autoreferat.ru