Обзор современных методов помехоустойчивого кодирования

П.В. Трифонов, профессор факультета безопасности информационных технологий, директор лаборатории теории информации и кодирования Университета ИТМО, редактор журнала IEEE Transactions on Communications, д.т.н.; pvtrifonov@itmo.ru
Б.Д. Кудряшов, профессор факультета информационных технологий и программирования Университета ИТМО, д.т.н.; bdkudryashov@itmo.ru
В.Д. Милославская, постдокторант-исследователь в области телекоммуникаций Школы электротехники и информационной инженерии, Сиднейский университет, к.т.н.; vera.miloslavskaya@sydney.edu.au

УДК 519.725, 621.391.1 DOI: 10.34832/ELSV.2021.19.6.007

Аннотация. *Рассмотрены методы помехоустойчивого кодирования, применяемые в современных системах передачи и хранения информации. Представлен краткий обзор кодовых конструкций, алгоритмов декодирования, достигаемых характеристик помехоустойчивости и производительности. Указаны основные достоинства и недостатки применяемых подходов, а также некоторые направления их развития.*

Ключевые слова: *помехоустойчивое кодирование, коды с малой плотностью проверок на четность, полярные коды, коды БЧХ, системы хранения данных.*

ВВЕДЕНИЕ

Теория кодирования за годы своего существования преобразовалась из раздела комбинаторики и алгебры в прикладную область знаний, с применениями которой мы сталкиваемся ежедневно. Внушительные успехи теории кодирования в последние десятилетия вплотную приблизили реальные системы связи к теоретическим пределам эффективности. В связи с этим стал весьма актуальным вопрос о перспективах дальнейшего развития теории. Цель приводимого ниже обзора – указать на «зазоры» между теорией и практикой и на те направления научных исследований, которые, по нашему мнению, составят фундамент систем связи будущих поколений.

ТУРБОКОДЫ И КОДЫ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

Изобретение турбокодов в 1993 г. [1] послужило началом нового этапа развития прикладной теории кодирования. Схема кодера неожиданно проста: два систематических сверточных кодера с общей информационной частью и перемежитель. Дальнейший анализ показал, что те же характеристики могут быть получены при использовании, например, произведения (итерирования) блоковых кодов [2].

Это означает, что основной выигрыш получен не за счет специальной конструкции кода, а за счет принципа итеративного декодирования. Это наблюдение способствовало привлечению внимания к работе Галлагера 1963 года [3], посвященной кодам с малой плотностью проверок на четность (МППЧ). Именно в этой работе сформулировано и математически обосновано применение принципа распространения доверия применительно к задаче декодирования по максимуму апостериорной вероятности. Работа [4], опубликованная в 1999 г., дала МППЧ кодам второе рождение. В настоящее время они стали основой многих стандартов связи.

В приложениях, ориентированных на системы беспроводной связи, предпочтение отдается МППЧ перед турбокодами в силу возможности распараллеливания вычислений. Элементарное введение в МППЧ коды можно найти в учебном пособии [5]. Введем обозначения, которые потребуются для описания конструкции МППЧ кодов.

Двоичный линейный (n, k)-код длины n размерности k может быть задан порождающей матрицей $\mathbf{G}$ размерности $k \times n$ либо проверочной матрицей $\mathbf{H}$ размерности $r \times n$, где $r = n–k$ – избыточность кода. МППЧ код задается порождающей матрицей, для которой введено ограничение на долю ненулевых символов. Для ансамблей МППЧ кодов мы требуем, чтобы с ростом длины кода количество единиц в строках и столбцах оставалось постоянным. Для используемых на практике МППЧ кодов среднее число единиц в столбцах матрицы находится в диапазоне от 3 до 4.

Галлагером в [3] доказано, что среди МППЧ кодов есть коды с минимальным расстоянием, растущим линейно с длиной кода. В более поздних исследованиях [6] менее строгим анализом установлено, что характеристики, близкие к пределу Шеннона, могут быть достигнуты даже при использовании субоптимального итеративного декодирования по принципу распространения доверия.

В стандартах связи используется подкласс МППЧ кодов – квазициклические (КЦ) МППЧ коды. КЦ МППЧ $(n = cM, k = bM)$-код со скоростью $R=k/n \geq 1-b/c$ задается проверочной матрицей вида

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_{11} & \mathbf{H}_{12} & \cdots & \mathbf{H}_{1c} \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{H}_{b1} & \mathbf{H}_{b2} & \cdots & \mathbf{H}_{bc} \end{pmatrix}, \quad (1)$$

где c, b – натуральные числа; квадратные подматрицы $\mathbf{H}_{ij}$ порядка M либо нулевые, либо представляют собой матрицы циклической перестановки вида $\mathbf{J}^{w_{ij}}$; $w_{ij} \in \{0, ..., M-1\}$ – целые числа, а $\mathbf{J}$ содержит ненулевой элемент в строке i только на позиции с номером $(i+1) \bmod M$. Например, при $M=4$

$$\mathbf{J} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Задача построения КЦ МППЧ кода сводится к поиску расположения ненулевых подматриц (выбор протографа) и значений степеней $\{w_{ij}\}$ матриц сдвига. Дополнительно накладывается ограничение на структуру протографа для обеспечения линейной сложности кодирования.

Одним из ориентиров при подборе матриц служит обхват соответствующего графа Таннера. С увеличением обхвата графа Таннера декодирование по принципу распространения доверия становится более эффективным. Но простое отбрасывание графов с короткими циклами не гарантирует высокой эффективности получаемых кодов. Асимптотически оптимальные распределения весов столбцов и строк проверочных матриц были найдены методами эволюции плотностей [6]. Один из подходов к оптимизации кодов конечных длин рекомендован в [7], там же подробно рассматриваются критерии для поиска кодов с хорошей корректирующей способностью.

Коды стандартов IEEE 802.11 (используются в Wi-Fi), IEEE 802.16, а также коды стандартов цифрового телевидения DVB используют проверочные матрицы вида (1). Недавно принятые в качестве кодов стандарта 5G КЦ МППЧ коды относятся к классу так называемых многореберных (multi-edge) кодов. В действительности структура матрицы осталась той же, что и прежде, но часть информационных символов не передается по каналу. Это сделано для снижения эффективной скорости передачи (для экономии энергии). Непереданные символы интерпретируются декодером как стертые и восстанавливаются на приемной стороне по остальным принятым символам. Еще одно отличие стандарта 5G состоит в способе формирования проверочной части матрицы. В предыдущих стандартах это была бидиагональная подматрица, а в новом стандарте 5G бидиагональная часть комбинируется с диагональной. Специальное кодирование из стандарта 5G заимствовано стандартом ATSC 3.0 [8], предназначенным для передачи сигналов цифрового телевидения.

Рисунок 1
Характеристики МППЧ кодов стандартов цифрового телевидения ATSC и DVB, n = 64800, вероятность ошибки на кодовое слово FER=10^{-4}

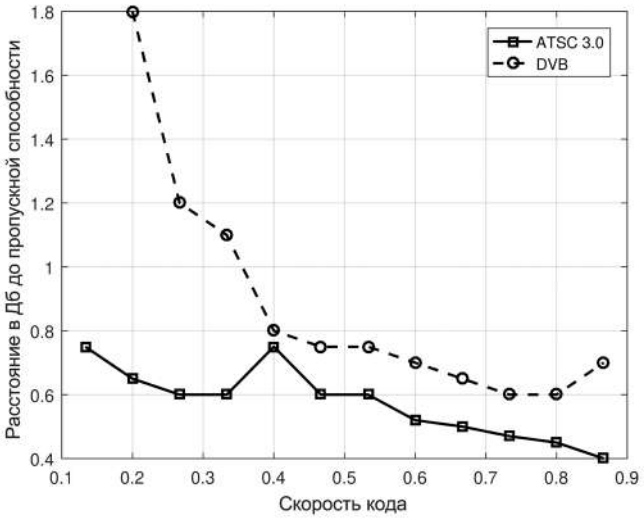
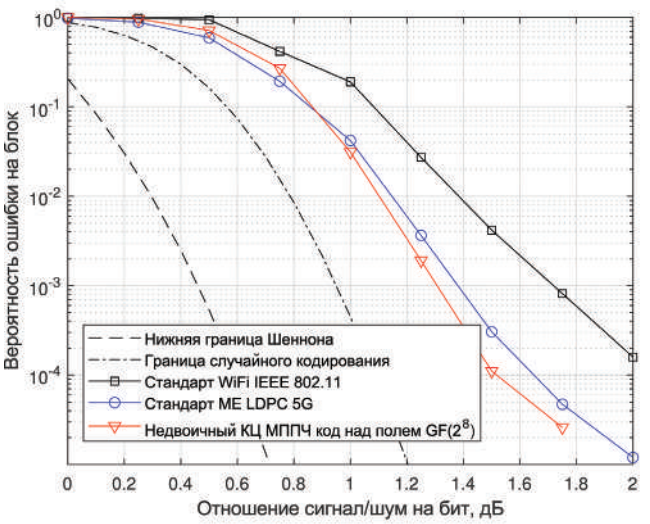


Рисунок 2
Характеристики КЦ МППЧ кодов стандартов беспроводной связи и недвоичных КЦ МППЧ, $n \approx 2000$, R =1/2



На рис. 1 и 2 показаны характеристики кодов из вышеуказанных стандартов. Как следует из графика на рис. 1, энергетическая эффективность длинных кодов стандартов цифрового телевидения находится всего в 0,4–0,6 дБ от теоретического предела. В качестве целевых показателей на рис. 2 мы привели нижнюю границу Шеннона [9] и границу случайного кодирования, подсчитанную с применением оценки Полтырева [10].

Граница случайного кодирования, хотя и является достижимой (верхней) границей вероятности ошибки, обычно рассматривается как предельно достижимая оценка вероятности ошибки, поскольку она достижима при отсутствии ограничений на структуру кода и при декодировании по максимуму правдоподобия (МП). Сравнение границ существующих кодов с теоретическими границами показывает, что коды из вышеуказанных стандартов отстоят от теоретических границ менее, чем на 0,4 дБ. Отметим особо, что результаты моделирования учитывают все реалистичные ограничения на сложность вычислений, точность представления данных и т.п.

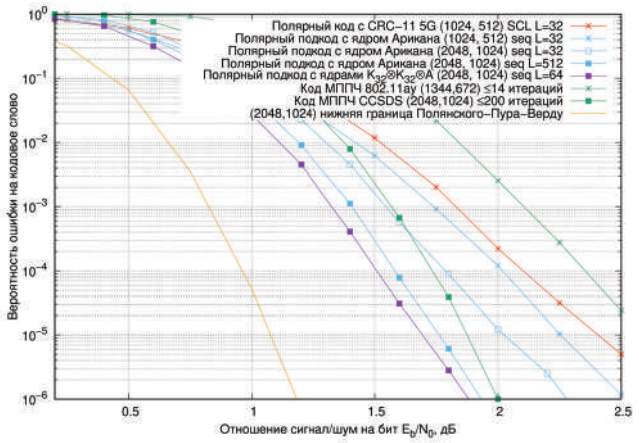
На рис. 2 приведены также результаты моделирования недвоичного КЦ МППЧ кода над полем Галуа GF(2^8), построенного в соответствии с алгоритмами, приведенными в [7]. Эти результаты показывают, что корректирующие коды, построенные над полями Галуа с числом элементов более двух, позволяют получить намного лучшую корректирующую способность по сравнению с двоичными кодами.

ПОЛЯРНЫЕ КОДЫ

Полярные коды были предложены в 2009 г. Э. Ариканом [11] и за 10 лет прошли путь до внедрения в стандарт мобильной связи 5G. Кодирование в полярном коде длины $n=2^m$ осуществляется путем вычисления вектора $\mathbf{c}=\mathbf{u}\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}^{\otimes m}$, где $\otimes m$ обозначает m-кратное произведение Кронекера матрицы с собой, часть символов вектора **u** содержит полезные данные, а остальные его элементы равны некоторым предопределенным значениям (например, 0). Это может быть выполнено со сложностью $\frac{1}{2}n\log_2 n$ операций. Существуют алгоритмы со сложностью $O(n)$ нахождения позиций в векторе **u**, пригодных для размещения полезных данных [12, 13]. Декодирование может быть выполнено с помощью алгоритма последовательного исключения (ПИ) со сложностью $n\log_2 n$. Полярные коды в сочетании с декодером ПИ обеспечивают сколь угодно надежную передачу данных со скоростью, меньшей пропускной способности соответствующего канала, т.е. достигают предела Шеннона.

Алгоритм ПИ не обеспечивает декодирование по МП. В связи с этим был предложен списочный алгоритм [14], который позволяет со сложностью $O(Ln\log_2 n)$ найти L кодовых слов, вычислить меру их близости к принятой последовательности и выбрать наиболее вероятное из них. Уже при небольшом размере списка L этот алгоритм обеспечивает декодирование полярных кодов почти по МП. Он может быть реализован в области логарифмических отношений правдоподобия с использованием только операций сложения и сравнения [15]. В отличие от кодов МППЧ, это приводит к крайне незначительному (менее 0,1 дБ) ухудшению корректирующей способности по сравнению с оптимальной реализацией. Описана аппаратная реализация этого алгоритма, обеспечивающая производительность до 3,25 Гбит/с на коде длины 1024 [16].

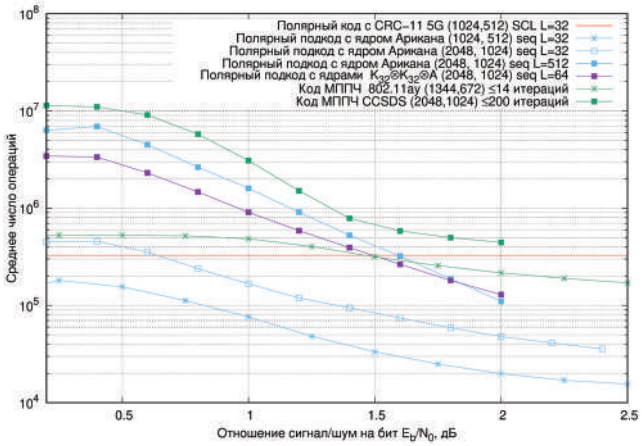
Рисунок 3
Корректирующая способность полярных и МППЧ кодов



Минимальное расстояние классических полярных кодов может быть оценено как $O(\sqrt{n})$, хотя известны семейства кодов, для которых оно растет линейно с увеличением длины. В связи с этим классические полярные коды не обеспечивают приемлемую корректирующую способность даже при использовании списочного декодера Тала-Варди. Поэтому получили распространение усовершенствованные конструкции. В частности, перед кодированием полярным кодом к данным может быть добавлена контрольная сумма CRC (cyclic redundancy check), а на стороне приемника из списка должны быть удалены все кодовые слова с неправильным значением контрольной суммы [14]. Уже это позволяет получить корректирующую способность лучше, чем у многих известных кодов МППЧ. Следует отметить, что CRC широко используется в протоколах физического уровня, поэтому такая модификация является почти «бесплатной». Еще лучшая корректирующая способность может быть получена, если часть символов вектора **u** на стороне передатчика положить равными сумме некоторых других его символов [17, 18]. Получаемые таким образом коды называются полярными подкодами. Комбинация этих решений была принята для использования в стандарте 5G.

Размер списка L, требуемый для обеспечения приемлемой корректирующей способности полярными подкодами и полярными кодами с CRC, растет с их длиной. В связи с этим, а также со значительной задержкой алгоритма ПИ и его аналогов, в стандарте 5G полярные коды рекомендованы для использования на длинах $n \le 1024$. Предложены обобщения полярных кодов, известные как полярные коды с большими ядрами [19], которые

Рисунок 4
Сложность декодирования полярных и МППЧ кодов



уже при небольших размерах списка L одновременно обеспечивают меньшую сложность и лучшую корректирующую способность по сравнению с полярными (под)кодами Арикана [20]. Кроме того, их корректирующая способность улучшается с увеличением длины заметно быстрее, чем в случае полярных кодов Арикана.

Следует особо отметить роль российской школы теории кодирования в развитии полярных кодов [21]. Идея преобразования канала, лежащая в основе полярных кодов, прослеживается в работе М.С. Пинскера [22]. Сами полярные коды являются частным случаем обобщенных каскадных кодов [23]. Четыре статьи российских исследователей, посвященные вопросам практического усовершенствования полярных кодов, включены в список IEEE Communications Society Best Readings in Polar Coding [12, 17, 24, 25].

На рис. 3 представлена вероятность ошибки декодирования методом Тала-Варди (SCL) и последовательным алгоритмом (seq) [24] некоторых полярных подкодов и кодов с CRC. Видно, что последовательный алгоритм обеспечивает существенно меньшую среднюю сложность декодирования. Полярный подкод, использующий два экземпляра ядра K_{32} размерности 32 и один экземпляр ядра Арикана A, показывает лучшие характеристики по сравнению с кодом с ядром Арикана.

На рис. 4 представлено среднее число арифметических операций, требуемое для декодирования рассмотренных кодов. Видно, что полярные коды допускают наиболее простое декодирование.

КОДЫ БЧХ И РИДА-СОЛОМОНА

Классические методы декодирования кодов Боуза-Чоудхури-Хоквингема (БЧХ) и Рида-Соломона, основанные на алгоритмах Берлекэмпа-Месси и Сугиямы, имеют сложность $O(nd)$, где d – минимальное расстояние кода. Она может быть снижена до $O(n\log(n–k)+(n–k)\log^2(n–k))$ за счет использования спектральных методов [26]. Благодаря исключительной простоте алгебраических декодеров этих кодов они находят свое применение в системах связи, предъявляющих особо высокие требования к производительности, а также как составная часть каскадных конструкций. В частности, эти коды предусмотрены стандартами IEEE 802.3bs и Open ROADM MSA 3.01 для оптических сетей со скоростью передачи данных до 400 Гбит/с.

Многие из этих систем предполагают использование мягкого декодирования. Наибольшее распространение получил декодер Чейза второго типа, представляющий собой надстройку над алгебраическим декодером [27]. На основе него может быть построен декодер с мягким выходом [2], применимый в итеративных декодерах каскадных кодов. Также описано применение алгоритма распространения доверия для декодирования кодов Рида-Соломона [28]. В [17] показано, что методы декодирования полярных кодов могут быть использованы для декодирования кодов БЧХ. Однако все эти приемы не позволяют выполнить декодирование кодов БЧХ по максимуму правдоподобия с приемлемой сложностью. В то же время известно, что расширенные примитивные коды БЧХ в узком смысле достигают предела Шеннона по крайней мере для двоичного стирающего канала [29], а на длинах до нескольких сотен символов они относятся к числу лучших по минимальному расстоянию. Таким образом, особую актуальность приобретает задача поиска простых алгоритмов декодирования кодов БЧХ, которые могли бы приблизиться к декодированию по максимуму правдоподобия.

КОДЫ ДЛЯ СИСТЕМ ХРАНЕНИЯ ДАННЫХ

В этом разделе мы рассмотрим применение методов помехоустойчивого кодирования в системах хранения данных (СХД), состоящих из нескольких устройств, например, дисков или серверов. Каждое отдельное устройство (узел) считается малонадежным и хранит не более одного элемента каждого кодового слова. Традиционным критерием выбора помехоустойчивого кода для СХД является минимизация избыточности при обеспечении заданного уровня надежности хранения данных. Этому критерию удовлетворяют коды с максимально достижимым кодовым расстоянием (МДР). При длине n и размерности k минимальное расстояние МДР-кода равно $d=n–k+1$. Для восстановления данных достаточно подключиться к любым k из n узлов, т.е. система устойчива к отказу любых $(n–k)$ узлов. Наиболее известными МДР-кодами являются коды Рида-Соломона, используемые в избыточных массивах независимых дисков (стандарт RAID-6 [30]), распределенной файловой системе Hadoop HDFS-EC, объектной системе хранения f4 BLOB компании Facebook, файловой системе Colossus компании Google и др.

МДР-коды позволяют минимизировать избыточность, однако объем трафика при восстановлении данных, хранимых на вышедшем из строя узле, оказывается весьма большим. Одной из первых кодовых

конструкций, решающих эту проблему, являются пирамидальные коды [31], разработанные для минимизации числа узлов, с которых необходимо считать информацию для восстановления данных, хранящихся на отказавшем узле. Пирамидальные коды не являются МДР-кодами, как и локально-декодируемые коды в целом [32–35]. Локальностью кода называют число символов кодового слова, которые необходимо считать для восстановления одного потерянного символа. Если все информационные символы имеют локальность r, то говорят, что информационная локальность равна r. Если все символы кодового слова имеют локальность r, то говорят, что полная локальность равна r. Построенный на базе $(n, k, n–k+1)$ кода Рида-Соломона пирамидальный код с информационной локальностью r имеет параметры $(n+\lceil k/r \rceil-1, k, n-k+1)$. Схожая кодовая конструкция с полной локальностью r имеет параметры $(n+\lceil n/r \rceil-1, k, n-k+1)$. В [32] было показано, что длина линейного кода $n \geq k(r+1)/r+d-2$ при размерности k, минимальном расстоянии d и информационной/полной локальности r. Однако для достижения равенства в случае полной локальности r требуется чрезвычайно большой алфавит. Малые значения локальности r и низкая вычислительная сложность восстановления данных достигаются посредством проверочных символов, равных функциям малого числа информационных символов.

Другой важной характеристикой при восстановлении отказавшего узла является объем трафика, измеряемый как число считываемых с других узлов символов. Регенерирующие коды [36] позволяют сбалансировать объемы трафика и избыточности. Регенерирующие коды превосходят локально-декодируемые коды по соотношению трафик/избыточность благодаря переходу от кодовых слов, состоящих из n символов, к кодовым словам, состоящим из n векторов по α символов. Любых k узлов достаточно для восстановления всех информационных символов, при этом для восстановления одного отказавшего узла достаточно считать по β символов с любых t узлов, т.е. объем трафика равен $\gamma=\beta t$. Параметры этих кодов удовлетворяют условию [37]

$$B \leq \sum_{i=0}^{k-1} \min\{\alpha, (t-i)\beta\},$$

где B – общее число информационных символов. Особый интерес представляют два крайних случая: регенерирующие коды с минимальным хранением (MSR) и регенерирующие коды с минимальным трафиком (MBR), характеризуемые параметрами [36]

$$(\alpha_{MSR}, \gamma_{MSR}) = \left(\frac{B}{k}, \frac{Bt}{k(t-k+1)}\right),$$

$$(\alpha_{MBR}, \gamma_{MBR}) = \left(\frac{2Bt}{2kt-k^2+k}, \frac{2Bt}{2kt-k^2+k}\right).$$

Коды с минимальным хранением, например [38], лежат на границе Синглтона, как и МДР-коды. Подробная информация об этих классах кодов приведена в [39, 40].

ЗАКЛЮЧЕНИЕ

Разработанные за последние 70 лет кодовые конструкции и алгоритмы декодирования позволяют вплотную приблизиться к фундаментальным пределам (границы Шеннона и Полянского-Пура-Верду) систем передачи информации. Платой за улучшение корректирующей способности является сложность декодирования. Несмотря на значительный прогресс в области создания простых декодеров, требования к производительности современных систем связи зачастую вынуждают использовать субоптимальные решения. Поэтому остается актуальной задача разработки алгоритмов декодирования с малыми задержкой и сложностью.

В настоящее время известны различные кодовые конструкции, достигающие предела Шеннона. Однако корректирующая способность тех из них, для которых известны простые алгоритмы декодирования, улучшается достаточно медленно с увеличением длины кода. Это вынуждает использовать на практике чрезмерно длинные коды, что влечет увеличение задержки передачи данных. Поэтому чрезвычайно важной для практики задачей является поиск хорошо масштабируемых семейств кодов с простым декодированием.

СПИСОК ЛИТЕРАТУРЫ

1. Berrou, C. Near Shannon-limit error-correcting coding and decoding: Turbo codes / C. Berrou, A. Glavieux, P. Thitimajshima // Proceedings of IEEE International Communications Conference. – 1993. – P. 1064-1070.

2. Pyndiah, R.M. Near-optimum decoding of product codes: block turbo codes / R.M. Pyndiah // IEEE Transactions on Communications. – 1998. – Vol. 46, Issue 8. – P. 1003-1010.

3. Gallager, R.G. Low-density parity-check codes: Ph.D. thesis / R.G. Gallager. – MIT, 1963. – 90 p.

4. MacKay, D.J.C. Good error correcting codes based on very sparse matrices / D.J.C. MacKay // IEEE Transactions on Information Theory. – 1999. – Vol. 45, Issue 2. – P. 399-431.

5. Кудряшов, Б.Д. Основы теории кодирования: учебное пособие / Б.Д. Кудряшов. – СПб.: БХВ, 2016. – 400 с.

6. Richardson, T. Modern Coding Theory / T. Richardson, R. Urbanke. – Cambridge University Press, 2008. – 590 p.

7. Bocharova, I.E. Searching for binary and nonbinary block and convolutional LDPC codes / I.E. Bocharova, B.D. Kudryashov, R. Johannesson // IEEE Transactions on Information Theory. – 2015. – Vol. 62, Issue 1. – P. 163-183.

8. Kim, K.-J. Low-density parity-check codes for ATSC 3.0 / K.-J. Kim, S. Myung, S.-I. Park et al. // IEEE Transactions on Broadcasting. –2016. – Vol. 62, Issue 1. – P. 189-196.

СПИСОК ЛИТЕРАТУРЫ

9. Shannon, C.E. Probability of error for optimal codes in a Gaussian channel / C.E. Shannon // The Bell System Technical Journal. – 1959. – Vol. 38, Issue 3. – P. 611-656.

10. Poltyrev, G. Bounds on the decoding error probability of binary linear codes via their spectra / G. Poltyrev // IEEE Transactions on Information Theory. – 1994. – Vol. 40, Issue 4. – P. 1284-1292.

11. Arikan, E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels / E. Arikan // IEEE Transactions on Information Theory. – 2009. – Vol. 55, Issue 7. – P. 3051-3073.

12. Trifonov, P. Efficient design and decoding of polar codes / P. Trifonov // IEEE Transactions on Communications. – 2012. – Vol. 60, Issue 11. – P. 3221-3227.

13. Tal, I. How to construct polar codes / I. Tal, A. Vardy // IEEE Transactions on Information Theory. – 2013. – Vol. 59, Issue 10. – P. 6562-6582.

14. Tal, I. List decoding of polar codes / I. Tal, A. Vardy // IEEE Transactions on Information Theory. – 2015. – Vol. 61, Issue 5. – P. 2213-2226.

15. Balatsoukas-Stimming, A. LLR-based successive cancellation list decoding of polar codes / A. Balatsoukas-Stimming, M.B. Parizi, A.P. Burg // IEEE Transactions on Signal Processing. – 2015. – Vol. 63, Issue 19. – P. 5165-5179.

16. Tao, Y. A configurable successive-cancellation list polar decoder using split-tree architecture / Y. Tao, S. Cho, Z. Zhang // IEEE Journal of Solid-State Circuits. – 2021. – Vol. 26, Issue 2. – P. 612-623.

17. Trifonov, P. Polar subcodes / P. Trifonov, V. Miloslavskaya // IEEE Journal on Selected Areas in Communications. – 2016. – Vol. 34, Issue 2. – P. 254-266.

18. Trifonov, P. A randomized construction of polar subcodes / P. Trifonov, G. Trofimiuk // Proceedings of 2017 IEEE International Symposium on Information Theory. –IEEE, 2017. – P. 1863-1867.

19. Korada, S.B. Polar codes: Characterization of exponent, bounds, and constructions / S.B. Korada, E. Sasoglu, R. Urbanke // IEEE Transactions on Information Theory. – 2010. – Vol. 56, Issue 12. – P. 6253-6264.

20. Trofimiuk, G. Reduced complexity window processing of binary polarization kernels / G. Trofimiuk, P. Trifonov // Proceedings of IEEE International Symposium on Information Theory. – IEEE, 2019. – P. 1412-1416.

21. Arikan, E. On the origin of polar coding / E. Arikan // IEEE Journal on Selected Areas in Communications. – 2016. – Vol. 34, Issue 2. – P. 209-223.

22. Пинскер, М.С. О сложности декодирования / М.С. Пинскер // Проблемы передачи информации. – 1965. – Т. 1, № 1. – С. 113-116.

23. Блох, Э.Л. Кодирование обобщенных каскадных кодов / Э.Л. Блох, В.В. Зяблов // Проблемы передачи информации. – 1974. – Т. 10, № 3. – С. 45-50.

24. Trifonov, P. A score function for sequential decoding of polar codes / P. Trifonov // Proceedings of 2018 IEEE International Symposium on Information Theory. – IEEE, 2018. – P. 1470-1474.

25. Trofimiuk, G. Efficient decoding of polar codes with some 16x16 kernels / G. Trofimiuk, P. Trifonov // Proceedings of 2018 IEEE Information Theory Workshop. – IEEE, 2018. – P. 1-5.

26. Lin, S.-J. FFT algorithm for binary extension finite fields and its application to Reed-Solomon codes / S.-J. Lin, T.Y. Al-Naffouri, Y.S. Han // IEEE Transactions on Information Theory. – 2016. – Vol. 62, Issue 10. – P. 5343-5358.

27. Chase, D. Class of algorithms for decoding block codes with channel measurement information / D. Chase // IEEE Transactions on Information Theory. – 1972. – Vol. 18, Issue 1. – P. 170-182.

28. Bellorado, J. Low-complexity soft-decoding algorithms for Reed-Solomon codes – Part II: Soft-input soft-output iterative decoding / J. Bellorado, A. Kavcic, M. Marrow, L. Ping // IEEE Transactions on Information Theory. – 2010. – Vol. 56, Issue 3. – P. 960-967.

29. Kudekar, S. Reed-Muller Codes achieve capacity on erasure channels / S. Kudekar, S. Kumar, M. Mondelli et al. // IEEE Transactions on Information Theory. – 2017. – Vol. 63, Issue 7. – P. 4298-4316.

30. Common RAID disk data format specification v2.0. – SNIA, 2009.

31. Huang, C. Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems / C. Huang, M. Chen, J. Li // ACM Transactions on Storage. – 2013. – Vol. 9, Issue 1. – P. 79-86.

32. Gopalan, P. On the locality of codeword symbols / P. Gopalan, C. Huang, H. Simitci, S. Yekhanin // IEEE Transactions on Information Theory. – 2012. – Vol. 58, Issue 11. – P. 6925-6934.

33. Yekhanin, S. Locally decodable codes / S. Yekhanin // Foundations and Trends in Theoretical Computer Science. – 2012. – Vol. 6, Issue 3. – P. 139-255. – http://dx.doi.org/10.1561/0400000030.

34. Tamo, I. Bounds on the parameters of locally recoverable codes / I. Tamo, A. Barg, A. Frolov // IEEE Transactions on Information Theory. – 2016. – Vol. 62, Issue 6. – P. 3070-3083.

35. Kruglik, S. New bounds and generalizations of locally recoverable codes with availability / S. Kruglik, K. Nazirkhanova, A. Frolov // IEEE Transactions on Information Theory. – 2019. – Vol. 65, Issue 7. – P. 4156-4166.

36. Dimakis, A.G. Network coding for distributed storage systems / A.G. Dimakis, P.B. Godfrey, Y. Wu et al. // IEEE Transactions on Information Theory. – 2010. – Vol. 56, Issue 9. – P. 4539-4551.

37. Wu, Y. Deterministic regenerating codes for distributed storage / Y. Wu, R. Dimakis, K. Ramchandran // In Allerton Conference on Control, Computing, and Communication, 2007.

38. Ye, M. Explicit constructions of high-rate MDS array codes with optimal repair bandwidth / M. Ye, A. Barg // IEEE Transactions on Information Theory. – 2017. – Vol. 63, Issue 4. – P. 2001-2014.

39. Круглик, С.А. Теоретико-информационный подход в задаче надежного распределенного хранения информации / С.А. Круглик, А.А. Фролов // Информационные процессы. – 2020. – Т. 20, № 1. – С. 22-40.

40. Ramkumar, V. Codes for distributed storage; edited by W.C. Huffman, J.-L. Kim, P. Sole / V. Ramkumar, M. Vajha, S.B. Balaji et al. // Concise Encyclopedia of Coding Theory. – Chapman and Hall/CRC, 2021.

Получено 15.02.21