

В редакцию журнала
«Проблемы передачи информации»

Уважаемая редакция!

Внимательно прочитал и проанализировал вполне конструктивную рецензию на мою статью «Каскадные схемы декодирования на основе недвоичных МПД». Прошу вас рассмотреть откорректированный с максимально возможным учётом мнения рецензента второй вариант статьи и передать рецензенту направляемый вам ответ.

Мне несколько странно, что рецензия начинается с утверждения, что *«Статья посвящена экспериментальным результатам и не содержит теоретического анализа алгоритма декодирования.»*. Наверное, у нас с рецензентом совершенно несовпадающий опыт работы по темам, которые интересны и в теоретическом, и в прикладном плане. Я склонен полагать, что разделы 1-3 статьи следует отнести к теоретическим, поскольку там описан алгоритм и даны нижние оценки его характеристик, которые достаточно точны, удобны для вычислений и для последующего анализа полученных результатов. Там же указаны ссылки на ещё более детально рассмотренные оценки характеристик этого типа. Кроме того, там же приведены и ссылки на оценки другого типа (верхние), что при ограниченном размере статьи, как мне кажется, вполне допустимо и даже является единственно возможным вариантом изложения. Это позволяет ещё до обсуждения каких-либо экспериментальных данных составить первое, но достаточно содержательное впечатление о возможностях метода. Но я готов далее не обсуждать это несколько странное начало отзыва, если рецензент всё же настаивает на этом пункте.

Далее, выражаю своё полное согласие с рецензентом в том, что *«... коды Рида-Соломона - это короткие коды...»*. Но эти слова написаны в том абзаце, где рецензент также полагает, что *«...экспериментальное сравнение с декодерами кодов Рида-Соломона не является правомерным, ...»*. Более того, абзацем выше рецензент пишет: *«Принципиальным недостатком работы является отсутствие сравнения полученных экспериментальных результатов с результатами доступными аналогичным современными практическими методами декодирования. А именно недвоичным LDPC кодам (кодам с низко-плотностной проверочной матрицей) и недвоичным турбо-кодам.»*.

По этому непростому вопросу мне хотелось бы указать на следующие обстоятельства. Я готов согласиться с тем, что читатели вашего научного издания в гораздо меньшей степени соприкасаются с вопросами практической реализации алгоритмов декодирования и их конкретными численными характеристиками, чем специалисты, читающие журналы по телекоммуникациям. Собственно поэтому я и привёл данные по своему новому алгоритму, относящемуся к открытиям в области теории кодирования (желательно с этим согласиться!), и по классическим декодерам для кодов Рида-Соломона (РС). Очевидно, что предложенный в статье материал для оценок экспериментальных данных вполне содержателен, поскольку мной были подготовлены графики возможностей алгоритма МПД и кодов РС для различных длин кодов, кодовых скоростей и размеров алфавита. И я вынужден указать, что во многих зарубежных публикациях **сопоставление с кодами РС почему-то оказывается вполне допустимым** (в том числе и турбо кодов или кодов LDPC!) и позволяет предъявлять

новые результаты научной общественности. Но почему я не могу поступить так же, как и авторы уважаемых зарубежных журналов, мне совершенно неясно!

В качестве частичного объяснения такого отношения к представленным мной экспериментальным данным могу указать (конечно, только предположительно), что это связано с тем, что недвоичные LDPC ещё неполно исследованы, их реальных характеристик ещё мало и вопросы сложности пока слабо проработаны. Именно поэтому наибольшее число публикаций этого типа относятся к LDPC кодам с $q=4 \div 16$ и лишь иногда с $q=256$. Если ещё учесть, что сложность декодера LDPC часто имеет порядок q^2 , иногда $q \cdot \log q$, а характеристики относятся к обычным каналам с ФМ2 или с КАМ модуляцией, где получить хорошие характеристики зачастую проще, чем в q -ичных симметричных каналах (qSC), то становится понятным почему сложно найти хорошие характеристики LDPC для сравнения моих МПД алгоритмов и недвоичных LDPC: последние очень сложны для больших шумов в qSC каналах и неэффективны именно там, где предложенные мной методы особенно просты и сходятся для qSC каналов к решениям оптимальных (переборных!) декодеров (ОД): для длинных кодов с большими значениями q . Коротко говоря, человек, решивший, что всё в этой сфере известно и можно просто взять и сравнить, реально не увидит многих характеристик, которые могут быть интересны. К этому можно только добавить, что я во всех статьях по q -ичным МПД специально использую коды с большими значениями q , что улучшает их корректирующую способность и значительно ускоряет работу, а сложность q -ичных LDPC декодеров в этом случае, наоборот, растёт даже существенно быстрее, чем q . **Невыигрышные характеристики не публикуются!**

Мне представляется в связи с этим, что вынужденно заниматься составлением обзоров по кодированию (которых, конечно же, просто недопустимо мало!) не должно входить в обязанность авторов оригинальных статей по конкретным алгоритмам. Сведения, изложенные в двух предыдущих абзацах, как мне кажется, должны быть доступны и известны всем специалистам по кодированию. Я веду достаточно широкую образовательную деятельность, но на добровольных общественных началах.

Ещё более непонятно мне замечание рецензента про турбо коды. По меньшей мере в части из них **(как известно!)** используются те или иные модификации алгоритма Витерби (АВ) и специальных свёрточных кодов. Автор обсуждаемой статьи фактически в каждой публикации по недвоичным МПД, подчёркивая важность этих исследований, указывает, что эффективный АВ для недвоичных кодов при больших значениях q создать просто невозможно. Поэтому реально в цифровой технике используются пока только короткие коды РС. Именно с этим и связано отсутствие публикаций с действительно высокими характеристиками помехоустойчивости и для турбо кодов, особенно (опять же!) при больших q в каналах типа qSC, когда именно МПД оказываются особенно эффективными. С этим как раз и связаны новые предложения автора статьи по применению QМПД в базах данных, где работа с байтами и более длинными словами (четыре байта – машинное слово – $q=10^9$ и более!) - это самый обычный и быстрый режим. Здесь же можно было бы обратить внимание на графики в статье и на то, что эффективность QМПД декодера огромна, а набор статистики порядка 10^{10} битов и более на обычных ПК – дело примерно на час, что есть и одновременное доказательство экстремальной простоты метода, который предполагается опубликовать!

Более того, хотелось бы подчеркнуть, что я для столь небольшой статьи ещё провожу и сравнение с алгоритмами для кодов РС, которые как бы относятся к «новым и хорошим» модификациям «списочных» декодеров (Судана и пр.) со сложностью порядка n^3 . На стр.11 и стр.12 для таких алгоритмов мной было указано, в частности, что при этом увеличение среднего числа исправляемых ошибок составляет порядка 5% и практически вообще не улучшает сколько-нибудь заметно эффективность применения кодов РС, тогда как сложность коррекции с этими алгоритмами возрастает для длинных кодов очень существенно, видимо, на несколько порядков.

Я очень надеюсь, что выполненная мной в этом ответе незапланированная огромная дополнительная работа будет принята во внимание и другие излишние требования ко мне и к статье более предъявляться не будут.

Наконец, я уже просто вынужден напомнить, что многие вопросы по сопоставлению методов освещены в моей монографии, а писать обзор по кодам всех типов ради очевидных и просто описанных результатов по МПД методам в небольшой статье было бы верхом неразумности. Нелишне также указать, что в тех же **зарубежных публикациях многие методы описаны вообще безо всякого сравнения с другими алгоритмами** и, тем не менее, публикуются, если в них есть разумное рациональное зерно. Это позволяет утверждать, что методы МПД, которые для некоторых наборов типичных параметров оказываются эффективнее кодов РС при сложности декодирования, как указано в статье, по порядку величины \sim в 10^9 раз меньшей, безусловно, заслуживают публикации как чрезвычайно простые итеративные алгоритмы с очень хорошей сходимостью к оптимальному переборному (!) решению.

Автор готов многократно соглашаться с многомерностью проблемы сопоставления алгоритмов и также желает видеть больше материалов по реальным характеристикам различных декодеров. Однако обзоров по методам кодирования в российской научной периодике почти нет. Не очень много обзоров и за рубежом. Рецензент и все желающие могут просмотреть обзоры по кодированию, подготовленные на нашем специализированном веб-сайте ИКИ РАН по кодированию www.mtdbest.iki.rssi.ru, содержащем более 250 блоков информации: статей, презентаций, демопрограмм, методов кодирования, лабораторных работ и ответов на вопросы по кодам. Вне всякого сомнения, любой другой обзор, возможно, несовпадающий с мнениями авторов публикаций на сайте, также может быть помещён на этот сайт просто в целях расширения представленного на нём спектра мнений. Можем указать также наш обзор по кодам в журнале «ЦОС», №1, 2008.

Наконец, отметим, что на указанном сайте, уникальном для нашей страны сетевом ресурсе по кодам, представлено большое число демопрограмм различных методов кодирования. Никто в нашей стране не владеет всеми основными современными методами кодирования, развитие которых обязаны, на самом деле, отслеживать квалифицированные коллективы специалистов. Это может только мой научный коллектив. Эти методы реализованы программно, во-первых, совместно с двумя специализированными имитаторами спутниковых каналов связи с гауссовским шумом различной интенсивности, в составе которых есть декодеры Витерби до длин порядка $K \sim 18$ (!), МПД, турбо коды и другие алгоритмы. Кроме того, дополнительно в учебных и тестовых целях на образовательной страничке нашего сайта также представлены МПД декодеры с особо высоким быстродействием, классические

декодеры для кодов РС, LDPC и иные алгоритмы. У нас есть и два аппаратных стенда для тестирования и демонстрации работы декодеров. Их ассортимент будет расти и в дальнейшем. Кстати, именно из реальных характеристик кодов РС следует **тот же вывод, что сделал и рецензент**: «...коды РС - это короткие коды...». Стоит только добавить, что длинные коды РС, конечно, тоже есть, но их сложность быстро растёт, а эффективность увеличивается чрезвычайно мало. Собственно поэтому QMPC алгоритмы и оказываются **действительно открытиями** (!) в техники коррекции ошибок в символьных данных, поскольку имеют несравненно лучшие возможности по сравнению со всеми другими методами по сложности (быстродействию) и эффективности – практически оптимальное декодирование по качеству при линейной от длины блока сложности. Подчеркнём наконец, что из-за огромных технических трудностей до сих пор в реальных проектах различных западных компьютерных фирм по-прежнему фигурируют только коды РС! Это относится к CD-, DVD- дискам, другим перспективным накопителям, и к базам данных. Прочих методов (турбо и LDPC) нет и в проектах! И именно поэтому роль QMPC невозможно переоценить.

Мне представляется, что указанные выше веб-ресурсы для сравнения алгоритмов помогут всем желающим оценить реальности соотношения характеристик декодеров. Я полагаю также, что только наш коллектив специалистов, разрабатывающий среди всей номенклатуры перечисленных выше алгоритмов ещё и MPC декодеры, имеет **реальное представление о соотношениях сложностей** при различных вариантах реализации. Имея огромный несопоставимый с другими коллективами опыт создания программных декодеров многих типов, мы непосредственно участвовали также в создании аппаратных декодеров MPC, Витерби, турбо и LDPC на программируемых современных кристаллах Xilinx и Altera. В связи с этим мы всегда готовы ко всем возможным вариантам конструктивного сотрудничества по любым теоретическим и прикладным вопросам кодирования. Но я предлагаю аккуратнее относиться к предлагаемым нами материалам для публикаций, поскольку, скорее всего, по многим рассматриваемым вопросам, включая сложность декодирования, наше мнение может быть, а **иногда и должно быть** (!) весьма весомо.

Если рецензент может учесть представленные выше соображения и согласится с моим предложением оставить сопоставление алгоритмов «как есть», то далее я перечисляю те корректировки текста, на необходимость которых он справедливо указал.

П1. Да, «Символ» заменён на «сообщение».

П2. Абзац отредактирован по-другому.

П3. Прошу рецензента снять этот пункт замечаний. Самоортогональные (иногда в те 70-е годы писали также: «собственно ортогональные») коды (тогда, разумеется, только двоичные) были предложены многими авторами: Месси, Робинсоном и Бернштейном, Ву (W.W.Wu), и пр. Они были также приведены в переводных книгах (Кассаами и др, Питерсон&Уелдон), где также рассматривались их свойства, согласно которым в силу построения они действительно содержали кодовые слова минимального веса с единственным ненулевым информационным символом. Есть эти коды и советской технической литературе 70-80-х годов. Скорее всего, придуманный пример рецензента не входит в этот класс кодов. Стараясь избежать и так уже затянувшейся дискуссии, предлагаю этот вопрос не обсуждать. И могу подтвердить, что во всех кодах этого типа я действительно пользуюсь тем, что кодовое слово минимального веса и в блоковом, и в свёрточном кодах всегда имеет один информационный символ. Это

удобно использовать при простых оценках вероятностей ошибки на символ или бит для оптимального декодера (ОД). Возможно, в той области, где работает рецензент, термин «самоортогональный (СОК)» имеет и другую смысловую нагрузку. Готов далее не обсуждать этот вопрос.

П.4. Если договорённость по терминологии в П.3 достижима, то этот пункт также снимается, а термин СОК добавлен в некоторых местах, в частности, где рецензент требует уточнить тип кода, в П.10 рецензии.

П.5. Да, согласен. Действительно, буквенных обозначений не хватает. Если это допустимо, предлагаю для избежания крупных переделок оставить символ “Q” для принятого сообщения, а «q» - для размера алфавита. Тем более что после раздела с основной теоремой символ «Q» больше не используется, а единый термин-сокращение QМПД также не мешает изложению материала.

П.6. Эти обозначения упорядочены.

П.7. Действительно, обсуждения свойств проверочной матрицы есть в разных местах текста, а её обозначение - «H» - пропущено. Исправлено.

П.8. Для более ясного понимания алгоритма и леммы 1 перед ней добавлен абзац о смысле синдрома S. Возможно, это упростит и улучшит восприятие последующего материала.

П.9. Первое предложение отредактировано.

П.10. Во всех экспериментах использовались самоортогональные коды (СОК) с малым уровнем размножения ошибок (РО). Эти сведения указаны в соответствующих местах разделов, относящихся к описанию экспериментальной части работы.

Мне представляется также, что мои вынужденные по сложившейся ситуации ссылки на реализации различных демо алгоритмов на нашем веб-сайте также будут приняты как полезные.

Я полагаю, что проработка указанных десяти пунктов замечаний (конечно, с учётом моих комментариев по поводу сложной проблемы сопоставления декодеров) позволит изменить мнение редакции и рецензента о возможности публикации представленной статьи. Хотелось бы надеяться также, что понимание с обеих сторон важности и сложности проблемы сопоставления привлечёт внимание специалистов, занятых чисто теоретическими исследованиями, к более реалистическим постановкам задачи максимально эффективного декодирования при очень небольшой фактической сложности алгоритмов коррекции ошибок.

Автор