О СОПОСТАВЛЕНИИ НОВЫХ МЕТОДОВ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

д.т.н., проф. Золотарёв В.В.[1], д.т.н., проф. Овечкин Г.В.[2]

[1]Институт космических исследований РАН
[2]Рязанский государственный радиотехнический университет

Анализируется эффективность известных методов коррекции ошибок для блоковых кодов в двоичных гауссовских каналах, в каналах со стираниями и в q-ичных симметричных каналах. Особое внимание уделено методам декодирования широко обсуждаемых в публикациях полярных кодов, а также низкоплотностных кодов, многопороговым декодерам (МПД) самоортогональных кодов и блоковой модификации алгоритма декодирования Витерби для коротких сверточных кодов. Наряду с вероятностью ошибки на блок оценена их вычислительная сложность. Проведенный анализ ряда публикаций показал, что эффективность базовых методов декодирования полярных кодов длиной до нескольких тысяч битов достаточно далека от теоретических границ и оказывается сопоставимой с эффективностью МПД, обладающих значительно меньшей вычислительной сложностью. Лучшей эффективностью обладают списочные методы декодирования полярных кодов, но их сложность оказывается пропорциональной размеру списка, что существенно усложняет их использование в высокоскоростных системах связи. Многократно большей оказывается сложность декодеров полярных кодов при их использовании для декодирования кодов Рида-Соломона. В то же время имеющиеся результаты по МПД для символьных кодов, обладающих линейной от длины кода сложностью реализации, показывают, что с их помощью можно обеспечить более высокие уровни достоверности передачи и хранения данных.

Быстрое развитие техники декодирования, её заметное улучшение по различным параметрам требует регулярного анализа текущих возможностей известных и новых алгоритмов коррекции ошибок. Ниже рассмотрены возможности хорошо знакомых специалистам алгоритма декодирования Витерби (АВ) и многопорогового декодера (МПД) в блоковой модификации по сравнению с алгоритмами для полярных кодов (ПК) [1, 2, 6].

Сложившаяся к настоящему времени специальная подача материала по ПК, когда вместо битовых вероятностей ошибки $P_b(e)$ оцениваются вероятности ошибок на блок WER, которая гораздо менее привычна в публикациях по технике декодирования, создаёт для читателей немало трудностей при сравнении различных алгоритмов. Столь же несколько условны характеристики эффективности ПК, которые зачастую подаются без каких-либо комментариев как численные результаты.

В докладе даётся сопоставление различных алгоритмов декодирования в двоичном гауссовском канале для блоковых кодов, что позволит относительно реалистично оценить возможности основных наиболее хорошо изученных кодов по параметру WER. Видимо, наиболее проблемным вопросом в настоящий момент является сложность декодирования для полярных кодов. Он требует конкретного уточнения, например, с использованием данных для производительности алгоритмов для них на стандартных процессорах для персональных компьютеров. Кроме того, уже весьма длительное время полярные коды предъявляются различными авторами очень противоречиво, как, например, в [4],: "Полярные коды – первый класс кодов, достигающих пропускной способности канала при длине кода, стремящейся к бесконечности, имеющий сложность кодирования и декодирования $O(n\log n)$, где n – длина кода. Однако корректирующая способность полярных кодов с практически значимыми длинами оказывается значительно хуже, чем, например, в случае кодов с малой плотностью проверок на чётность (LDPC)". Обратим внимание на то, что такая рекомендация полярных кодов делает их вроде бы привлекательными по сложности, но тут же возникают вопросы о причинах малой эффективности даже по сравнению с низкоплотностными кодами. Отметим также, что предлагаемые обычно оценки сложности, не зависящие никак от уровня шума канала, да ещё оказывающиеся одного порядка для принципиально различных по предназначению процедур кодирования и декодирования смотрятся как весьма

проблематичные. Ещё одной особенностью ПК является отсутствие содержательных результатов по использованию этими методами свёрточных кодов. Указанные выше противоречивые комментарии относительно свойств ПК могли бы быть компенсированы при использовании именно свёрточных кодов, для которых показатель экспоненты надёжности именно при большом уровне шума оказывается существенно большим, чем у блоковых кодов. Это могло бы значительно улучшить эффективность ПК.

Ниже сравниваются возможности ряда известных кодов и алгоритмов их декодирования по эффективности и, пока очень условно, по сложности, что поможет специалистам лучше ориентироваться в реальностях известных и новых методов коррекции ошибок. Разумеется, более точные оценки и сравнительные характеристики алгоритмов и кодов класса ПК пока ещё в будущем, хотя довольно скоро мы будем отмечать десятилетие развития этого направления.

На рис. 1 представлены зависимости вероятности ошибки на слово (на блок) WER для разных двоичных блоковых кодов как функции от уровня шума гауссовского канала (АБГШ) E_b/N_0. Кривая S – оценка для эффективности наилучших из возможных блоковых кодов длины n=1024 с кодовой скоростью R=1/2. Она указывает на потенциальные возможности кодов такой относительно небольшой длины, которые можно, в принципе, достичь. Оценки получены методом сферической упаковки, следствием чего реальные WER кодов оказываются всегда существенно более слабыми. Именно это и демонстрируют далее при R=1/2 все методы, характеристики которых обсуждаются далее.

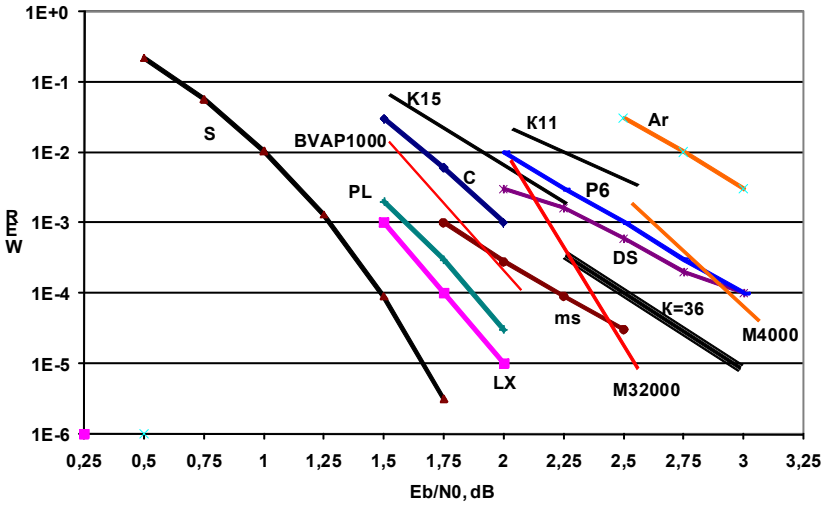

Рис. 1. Характеристики современных методов коррекции ошибок

Графики C, PL, ms, P6 и LX представляют вероятности WER полярных кодов длины n=1024, причём, для PL размер списка решений равен L=128, что весьма немало, а для LX он даже равен L=2048, что реально означает для небольших обсуждаемых значений n очень высокую неопределённость результата декодирования [6]. Остальные кривые относятся к кодам длины n~2048 или близким к ним. Далее для полярных кодов: график Ar согласно [5] относится к работе [1], кривая DS получена в [5] в соответствии с [3] при L=32, нижняя граница **ms** соответствует нескольким методам из [6] со списком до L=32, граница C относится к четырём методам из [4] со списком до L=32, использующим в составе каскадных ПК до девяти составляющих кодов. Ещё четыре результата из [2] можно ограничить снизу кривой P6.

Укажем другие уже хорошо изученные методы декодирования, которые применим без какой-либо специальной адаптации к условиям сравнения с характеристиками полярных кодов.

Результаты моделирования их работы в канале с АБГШ:

K15 – результат для блокового АВ [12] с порождающим полиномом свёрточного кода длины K=15 при длине блокового кода n=400. При этом скорость декодирования блокового АВ составляет 1000 бит/с на ноутбуке с процессором Core-i7, для которого будут приведены

характеристики производительности и для других алгоритмов. Отметим, что это весьма простой декодер, который был создан ещё в 1990 г. для проекта "Кассини" (полёт к Сатурну).

Далее, К11 – блоковый АВ при длине блока n=200 для K=11. Скорость декодирования при тех же условиях – 15 Кбит/с. Это очень простой АВ.

Наконец, обратим внимание на линию К36, которая относится к (единственная на графике!) к вероятности ошибки на бит $P_b(e)$ для свёрточного АВ с K=36 с просмотром всего лишь N=64 путей, как у классического совсем небольшого декодера АВ с K=7. График BVAP1000 соответствует оценке для блокового АВ с неполным просмотром путей. Его производительность пока оценивается величиной порядка 3000 бит/с.

Укажем на рис. 1 возможности методов МПД [7-9, 14]. Для кода с n=4000 битов приводится график М4000 с производительностью 230 Кбит/с, а для кода с n=32000 даётся график М32000 для декодера с производительностью 110 Кбит/с. Коды для МПД выбирались из имеющейся базы двоичных кодов без какой-либо специальной адаптации или особого выбора и для них был реализован стандартный обычный алгоритм МПД.

Рассмотрим далее соотношение общих свойств перечисленных выше алгоритмов декодирования. Начнём с того, что ситуация с полярными кодами (ПК) очень похожа на историю развития методов последовательного декодирования свёрточных кодов в 70-х годах прошлого века. Как известно, основные модификации алгоритмов этого направления не работают в гауссовском канале при уровне шума, большем вычислительной скорости канала R_1, когда, например, при R=1/2 это отношение E_b/N_0=2,5 дБ, что на 2,3 дБ хуже по энергетике, чем при пропускной способности канала C=1/2 [7]. При этом огромное количество статей в те годы анализировало статистические параметры распределения числа операций алгоритма, но реальные характеристики достоверности, конечно, представлявшие главный интерес, долгое время вообще было трудно отыскать где-либо. Различные модификации последовательных алгоритмов также в дальнейшем не смогли устранить их недостатки. Примерно такой же была и ситуация с кодами БЧХ, про которые было известно, что их возможности ещё более ограничены. Эти коды, например, при R=1/2 можно было применять, в основном, в обычном ДСК при вероятности ошибки в канале не более 0,037, что соответствовало уровню E_b/N_0>5 дБ, а их использование в гауссовском канале было сложной проблемой, которая не решалась даже при совместном использовании с ними других методов, например, Чейза (см. [7]).

Развитие алгоритмов для ПК также не лишено аналогичных особенностей и недосказанностей. Действительно невысокие характеристики эффективности ПК почти сразу с появлением этого нового направления в теории кодирования были "усовершенствованы" таким образом, что, аналогично уже хорошо отработанным методам для кодов Рида-Соломона (РС), решением декодеров ПК стали считать некоторый список возможных сообщений размера L, из которого в качестве результата декодирования выбирается сообщение, например, с выполняющимся CRC. Если истинное решение попадает в такой список, то декодирование считается успешным. Разумеется, размер L списков может составлять десятки и даже тысячи вариантов сообщений, что многократно снижает вероятность ошибки для этого удобного способа принятия решения, очень подходящего для теоретиков. Подчеркнём, что сложность такого модифицированного алгоритма растёт в этом случае также в L раз, что резко ухудшает и так невысокие технологические возможности ПК (сравните простейшие схемы кодирования и декодирования для вполне эффективных алгоритмов, рассмотренных в [7]).

При других подходах к декодированию ПК их изначально недостаточно высокие исходные характеристики улучшаются другими хорошо известными мощными средствами повышения эффективности кодирования и декодирования. К ним относятся обычные методы каскадирования, системы с обобщёнными каскадными кодами [10], а также целый спектр методов последовательного декодирования, адаптированных под потребности ПК. При этом удаётся строить ПК с более высокими значениями минимального кодового расстояния d, чем у исходных некаскадных методов, а применение итеративных подходов к их декодированию приводит к возможности работы при несколько более высоком уровне шума. Вместе с тем высокая неоднородность вычислений в декодерах таких ПК заметно усложняет и так идеологически совсем непростые средства кодирования/декодирования в сложных схемах такой обработки (см. кривую С для каскадного кода [4] с девятью (!) составляющими кодами!).

А применение итеративных методов для ПК при числе итераций порядка нескольких сотен, а иногда и существенно большем, чем 1000, уводит сложность их декодирования на уровни столь высокие, что обсуждение вопросов простоты реализации этих алгоритмов становится вообще неактуальным.

Далее отметим, что стиль полярных кодов для декодирования кодов РС реализуется алгоритмами, как указывают некоторые авторы [6], со сложностью $O(Ln^3 \log n)$. Возможно, что именно из-за высокой их сложности пока удалось найти опубликованные результаты в стиле ПК только для коротких кодов РС. Сравните эту ситуацию с результатами [7, 8, 9], где символьные коды большой длины декодируются с линейной от длины кода сложностью на тех же процессорах на скоростях от сотен Кбитов/с до Мбитов/с при большом уровне шума (демо программы могут быть переписаны с указанных выше ресурсов вместе с инструкциями по применению и затем проанализированы самостоятельно или с нашей поддержкой).

Ещё одна сфера применения ПК – для каналов со стираниями – также оказывается возможной, но всё же, как это было указано в [1], не столь эффективной, как хотелось бы. В [8] приведены характеристики МПД для таких каналов также при линейной от длины кода сложности алгоритмов восстановления, которые можно использовать для сравнения с [1]. Указанный МПД вполне эффективно работает даже при $R \sim 0{,}96C$, когда вероятность невосстановленных символов при $R=1/2$ в канале с вероятностью стираний $p_{ers} \sim 0{,}48$ не превышает уровня 10^{-6}. Результаты [8] вслед за публикациями по символьными кодам [9, 11, 14] фактически полностью закрывают ещё одну конкурентную сферу в теории и технике помехоустойчивого кодирования, где абсолютное преимущество, видимо, надолго, а возможно, что практически навсегда закрепляется за идеологией оптимизационной теории и конкретно за методами МПД в этих двух важнейших областях разработки алгоритмов декодирования.

Учитывая приведённые выше соображения, рассмотрим характеристики методов, приведённых на рис. 1. Напомним ещё раз, что, заявляя высокие характеристики декодирования ПК, абсолютное большинство этих кодов рассматривается для очень небольших длин, что и было уже отмечено выше. Но вполне очевидно, что для коротких кодов длины менее $n \sim 10^4$ об эффективной работе алгоритмов вблизи пропускной способности канала речи идти не может ни для каких кодов. При этом степень и скорость приближения характеристик любых алгоритмов к пропускной способности канала с ростом длины для разных классов кодов всегда весьма различны. Поэтому при небольших длинах кодов сравнение алгоритмов декодирования требует аккуратного анализа конкретных реализаций макетов алгоритмов для ПК. Демо программы для многих других классов кодов можно переписать с ресурсов [7] и затем анализировать при различных кодовых параметрах.

Начнём с того, что график Ar для исходного кода действительно показывает невысокие возможности ПК, предъявленные автором метода. Все конкурирующие с ним методы явно имеют существенно более высокие характеристики во всех вариантах выбранных реализаций АВ и МПД, причём последний метод декодирует свои коды с очень большой скоростью. Оба метода используют коды и большей и меньшей длины, чем 1024, что показывает хороший диапазон возможностей этих методов. Более того, реально простейшие по реализации и по структуре кодов АВ и МПД алгоритмы имеют фактически те же характеристики, что и классы методов, помеченных как P6 и DS, которые используют коды со сложной структурой, включающей каскадирование.

Оценки показывают, что применение простейших хорошо известных методов каскадирования к алгоритмам АВ и МПД, почти не снижающих их скорость работы, позволят уменьшить вероятность ошибки на блок этих методов примерно на 2 порядка. Это дополнительно улучшит вполне приемлемые характеристики указанных выше кодов, взятых для предварительного сравнения с без какого-либо специального подбора. Эти коды наряду с применением принципов дивергентного декодирования [13] успешно развиваются в простых эффективных сочетаниях и имеют широкие перспективы применения. Разумеется, некоторое непринципиальное уточнение ситуации с различными кодами по вопросам эффективности и сложности возможно при появлении достоверной информации по реализации алгоритмов для ПК. А пока что уже очень длительное отсутствие сколько-нибудь содержательных конкретных результатов по реализации декодеров для ПК только подтверждает довольно распространённое

мнение о неоправданной сложности алгоритмов декодирования по меньшей мере для ряда типов полярных кодов.

Вернёмся к рис. 1. Графики PL, LX, ms и C соответствуют различным методам, которые связаны со сложными итерациями алгоритмов для ПК, видимо, гораздо более сложными, чем у МПД. Кроме того, многие из них относятся к декодированию списками. Важно подчеркнуть, что введение списков – вынужденная мера, спасающая малоэффективные алгоритмы. Но их использование весьма затрудняет применение техники декодирования в реальных системах связи, когда непонятно как найти истинные сообщения в мешке возможных сотен "похожих" равновозможных данных, полученных из канала. Эти методы приёма "списком" должны всегда анализироваться только отдельно. Обычные методы декодирования, более соответствующие реальным системам телекоммуникаций, не должны сравниваться со списочными системами, поскольку это принципиально другая постановка задач кодирования, содержательность которых ещё нужно доказать или как-то оправдать.

Отметим далее, что граница BVAP1000 для блоковых модификаций AB с упрощённой реализацией показывает вместе с графиком K36, пока в виде оценок, характеристики ещё одного очень однородного и простого метода декодирования кодов небольшой длины. Его правильное использования вместе с простейшими методами каскадирования уже создали условия для реализации успешного простого декодирования недлинных сообщений при большом уровне шума.

В заключение отметим, что текущее состояние многолетних исследований структур и алгоритмов для полярных кодов всё ещё находится в состоянии затянувшегося первоначального этапа становления. До сих пор нет никаких оснований для утверждений, что появился эффективный и простой метод, применимый во многих реальных системах связи. Указанная выше сложность алгоритмов для кодов PC порядка $O(Ln^3 \log n)$ также не позволяет надеяться на скорое эффективное распространение этого подхода на недвоичные коды.

Текущее состояние прикладной теории и техники кодирования характеризуется хорошими уровнями эффективности и приемлемым уровнем сложности реализации LDPC кодов, а также быстрым и успешным развитием новых модификаций кодов и алгоритмов декодирования с прямым контролем метрики. Новые результаты для таких кодов позволят в ближайшее время уточнить соотношение их возможностей для гауссовских каналов. А абсолютное преимущество МПД алгоритмов по равнению с другими методами для недвоичных и стирающих каналов уже сформировалось и оказывается настолько существенным, что, видимо, оно закрепится за этими мощными системными средствами коррекции ошибок из арсенала оптимизационной теории кодирования на весьма длительную перспективу.

Литература

1. Arikan E. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. // IEEE Transactions on Information Theory, Vol. 55, No. 7, 2009, — C. 3051–3073.

2. Seidl M., Huber J.B. An Efficient Length- and Rate-Preserving Concatenation of Polar and Repetition Codes. // International Zurich Seminar on Communications (IZS), February 26 – 28, 2014.

3. Dumer I., Shabunov K. Soft-Decision Decoding of Reed–Muller Codes: Recursive Lists. // IEEE Transactions on Information Theory, Vol. 52, No. 3. – Март 2006. – C. 1260–1266.

4. Семёнов П.К. Декодирование обобщенных каскадных кодов с внутренними полярными кодами. // Информационно-управляющие системы, № 5 (60) / 2012 .

5. Морозов Р.А. Декодирование полярных кодов с помощью алгоритма Думера-Шабунова. // Реф.: spisok.math.spbu.ru/2013/txt/papers/s7_1.odt.

6. Милославская В.Д. Методы построения и декодирования полярных кодов. // Кандидатская диссертация. СПГПУ, 2014г., 206 с.

7. Золотарёв В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы. Справочник. М., «Горячая линия – Телеком», 2004, 126 с.

8. Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В., Аверин С.В., Овечкин П.В. - 25 лет оптимизационной теории кодирования: новые перспективы // **Пленарный доклад.** Материалы 18-й Международной научно-технической конференции "Проблемы передачи и обработки информации в сетях и системах телекоммуникаций", 2015, с.10–17.

9. Ресурсы **www.mtdbest.iki.rssi.ru**, **www.mtdbest.ru**.

10. *Блох Э., Зяблов В.* Обобщенные каскадные коды. М.: Связь,1976,240 с.

11. Золотарёв В.В., Чулков И.В., Овечкин Г.В., Сатыбалдина Д.Ж. Методы ускорения алгоритмов декодирования символьных кодов // Современные проблемы дистанционного зондирования Земли из космоса., М., ИКИ РАН, 2014, Т.11, №2, с.138–151.

12. Золотарёв В.В., Овечкин П.В. Характеристики декодирования блоковых кодов по алгоритму Витерби для систем ДЗЗ // XIII Всероссийская открытая конференция "Современные проблемы дистанционного зондирования Земли из космоса", М., ИКИ РАН. 2015.

13. Золотарёв В.В., Овечкин Г.В. Применение дивергентного кодирования в каналах спутниковой связи и ДЗЗ. // XIII Всероссийская открытая конференция "Современные проблемы дистанционного зондирования Земли из космоса", М., ИКИ РАН. 2015.

14. Золотарёв В.В., Зубарев Ю.Б., Овечкин Г.В. Многопороговые декодеры и оптимизационная теория кодирования. // Под редакцией академика РАН В.К. Левина. М., «Горячая линия – Телеком», 2012, 238 с.

ABOUT COMPARISON OF NEW METHODS FOR ERROR-CORRECTION

prof. Zolotarev V.V.[1], prof. Ovechkin G.V.[2]

[1]Space Research Institute
[2]Ryazan State Radioengineering University

The performance of known error correction methods for block codes over binary Gaussian, erasure and q-ary channels is analyzed. The work gives main attention to methods for decoding of polar codes widely discussed in periodic, low-density parity-check codes, multithreshold decoders for self-orthogonal codes and block modification of Viterbi decoder for short convolutional code. The word error rate (WER) performance and computational complexity of these methods are estimated. Analysis of publications shows the WER performance of base decoders for polar codes of length up to several thousand bits is far enough to theoretical bounds and is comparable to the performance of multithreshold decoders which one has much less complexity. Known list decoders for polar codes has better WER performance but their complexity is proportional to list size. It complicates application of such methods in high speed communication. The complexity of polar based decoders for Reed-Solomon codes is many times more in comparison even with list decoders. Yet known results on multithreshold decoding for non-binary codes shows than these decoders provide much mode reliability of data transfer and storage with linear complexity only.