

КРАТКИЕ СООБЩЕНИЯ

УДК 519.72

О ТРЕХ ЗНАЧИМЫХ ЮБИЛЕЯХ ТЕОРИИ КОДИРОВАНИЯ

Г. В. Овечкин, д.т.н., доцент, заведующий кафедрой ВПМ РГРТУ, Рязань, Россия;

orcid.org/0000-0001-6887-2217, e-mail: g_ovechkin@mail.ru

А. Н. Пылькин, д.т.н., профессор, профессор кафедры ВПМ РГРТУ, Рязань, Россия;

orcid.org/0000-0001-9925-2870, e-mail: pylkin.a.n@rsreu.ru

Рассматривается задача исправления ошибок при передаче данных по каналам с шумом, эффективное решение которой основывается на применении помехоустойчивых кодов и методов их декодирования. Целью работы знакомство читателя с основными этапами развития теории кодирования. Описаны наиболее значимые результаты, появление которых привело зарождению и развитию как классической теории кодирования, так и оптимизационной теории кодирования.

Ключевые слова: теория кодирования, оптимизационная теория кодирования, помехоустойчивые коды, двоичные коды, символьные коды, размножение ошибок, многопороговый алгоритм декодирования.

DOI: 10.21667/1995-4565-2024-90-153-157

Когда в 1948 году великий Клод Шеннон издал свою уникальную работу «Математическая теория связи» [1], она сначала не произвела особенного впечатления на его современников. Математики восприняли ее достаточно холодно. Бурные события в мире последних лет, наверное, также стали причиной того, что 75-летний юбилей этой действительно судьбоносной для будущего цифрового мира публикации не был достаточно широко отмечен и в прошедшем 2023 году. Тем не менее, ни с чем более не сравнимое значение этого результата Шеннона со временем только возрастает и становится все более значимым во многих прикладных аспектах, поскольку в тот год нашей цивилизации был указан путь в цифровой мир, который, как мы теперь осознаем, уже давно преобразует нашу жизнь во всех социальных, технических, научных, военных и, что несколько неожиданно для интеллектуальных достижений, даже в политических аспектах.

Шеннон в своей работе постулировал важнейшие необычные свойства новой теории, согласно которой для увеличения достоверности передачи цифровых данных в шумах, в отличие от аналогового сигнала, совершенно не требовалось увеличивать мощность передатчика. Следовало только выбрать особенную систему сигналов, что, как утверждал автор этой публикации, затем позволит при связи даже по каналам с весьма высоким уровнем шума, приводящим к искажениям при передаче отдельных компонентов цифрового потока, обеспечить сколь угодно высокую достоверность всего сообщения в целом на приемном конце линии связи. Так родилась теория помехоустойчивого кодирования (ТК).

Это был весьма неожиданный для инженеров тех лет результат. И сначала было не совсем ясно, как обрабатывать такое искаженное в канале с шумами сообщение. Иначе говоря, Шеннон доказал теорему существования, что для первой столь необычной публикации о сути цифрового мира было вполне допустимым вариантом вброса новой идеи про обработку цифровых данных. Но уже фактически через пару лет были открыты коды Хемминга [2], исправлявшие равно одну ошибку в двоичном цифровом блоке. И затем в течение десятка лет

специалисты как бы примерялись к цифровой проблематике, понемногу осознавая важность новой цифровой информатики.

А после 1960 г. всего за несколько лет математики создали обширные семейства двоичных алгебраических блочных кодов и алгоритмов их декодирования [3], которые уже могли стать основой аппаратуры формирования цифровых каналов, причем, что было крайне важным, со сложностью N , как число простейших операций, выполняемых алгоритмом при декодировании кодового блока длины n , т.е. с декодированием, пропорциональным всего лишь $n(\log n)^2$ и даже менее. Очень быстро появились и алгоритмы для недвоичных кодов Рида-Соломона (РС) [4]. Правда, у алгебраистов так и не нашлось кодов с линейной по n сложностью декодирования, что позже стало существенным препятствием для участия в конкурсе алгоритмов коррекции ошибок для различных типов каналов. Да и корректирующие способности этих кодов так и остались весьма умеренными, существенно ниже достижимой границы, которую указывала довольно быстро развивавшаяся во всех своих ключевых аспектах ТК. Тем не менее, ТК стала общепризнанной, причем для алгебраических кодов можно было вычислить сложность N .

Однако оптимальные, наилучшие по вероятности ошибки декодирования методы декодирования оказались совсем другими и сначала относились к непрерывным (сверточным) кодам, выдающимися представителями которых стали с 1967 г. алгоритмы Витерби (АВ) [5], оказавшиеся, однако, экспоненциально сложными относительно длины кода n , поскольку реализовали весьма элегантный переборный вариант обработки данных при движении декодера АВ по кодовой решетке сверточного кода. И при этом на самом деле реально достижимые оптимальные характеристики декодеров АВ даже при элементной базе того времени стали настоящим спасением прикладной ТК на многие десятилетия. Это определялось тем, что АВ практически без изменений сразу стал успешно работать и в двоичных гауссовских каналах, реализуемых в спутниковых и многих иных сетях, чему так и не научились никогда в приемлемой степени алгебраические коды. Так что к 1970 г. наступила первая фаза крайне странного в дальнейшем развития прикладной ТК – лидерство при создании систем связи захватил АВ, экспоненциально сложный метод. А к довольно слабым результатам математиков в алгебраической ТК возникли вопросы. Однако именно математические результаты, обязательно фиксируемые в формульном виде, тем не менее продолжали считаться целевыми достижениями ТК, тогда как инженеры предпочитали использовать именно АВ, а также пороговые декодеры сверточных кодов с очень простой реализацией. Ситуация в ТК становилась непростой и неоправданно странной.

Но, как оказалось, еще 50 лет назад МФТИ (второе выдающееся юбилейное событие!) запатентовал особый мажоритарный алгоритм декодирования [6] с линейной по n сложностью $N \sim n$. И более того, чрезвычайно быстро выяснилось, что этот метод, названный многопороговым декодированием (МПД), первый из эффективных алгоритмов с итеративным (при многократных попытках коррекции ошибок) декодированием на каждом шаге изменения символов в принятом сообщении всегда строго приближается к решению оптимального декодера (ОД). Линейная сложность МПД и его четко выраженное стремление к решению ОД, неизвестные ни у каких иных методов, сразу выделило алгоритмы МПД в новую параллельную и очень эффективную прикладную ТК. Однако реальное достижение МПД декодерами решений ОД оказалось возможным четко показать только в эксперименте, что совершенно не воспринималось теоретиками. На эти процессы оформления новой весьма технологичной прикладной теории, названной Оптимизационной Теорией (ОТ) помехоустойчивого кодирования, ушло около 10 лет.

И ТК как бы раскололась надвое, но каким-то очень странным образом. Теоретики строили свои просчитываемые, но слабые конструкции. Но ведь и итеративная коррекция мажоритарно декодируемых двоичных кодов была опробована почти сразу после открытия таких кодов американским ученым Дж. Месси [7] и оказалась совершенно неэффективной. Однако школа ОТ за несколько лет решила именно оптимизационными методами сложнейшую про-

блему размножения ошибок (РО) в мажоритарных декодерах [8], к которой за 60 лет развития ТК математиками даже не смог корректно приблизиться ни один научный коллектив в мире! И на основе теории РО действительно в ОТ полностью решена проблема эффективности МПД, которые стали достигать на новых кодах, построенных согласно теории РО, решений ОД!

Но создание ОТ на самом деле разделило адептов двух теорий по гораздо более жесткому принципу. Высочайший уровень сходимости решений МПД в рамках ОТ обусловлен и тем, что сложность алгоритмов ОТ (число простейших операций декодера) линейная, $N \sim n$ при практически гарантированном достижении решения ОД. И полувековое развитие такой ОТ параллельно с прежней ТК, неспособной обойтись без формул, полностью развело их методически по разным технологиям и идеологиям. ОТ четко ориентировалась на оптимизационные методы, учитывая, конечно, допустимые границы для итоговой эффективности, быстро искала все новые модификации МПД. А работы прежней ТК осложнялись тем, что там, считали, что оптимальными могут быть только переборные алгоритмы типа АВ. Им оказалось удобным считать, что ОТ – это просто некоторые программистские забавы.

Но уже совсем неразрешимой проблемой для «той» ТК, сворачивавшей свою деятельность, было то, что на самом деле среди теоретиков никто и нигде так и не смог вычислить вероятности ошибки и сложность своих каких-либо декодеров при достаточно большом уровне шума, когда к.п.д. используемых каналов оказывается, естественно, наибольшим и где как раз и надо применять хорошие коды. Все это полностью относится и к ОТ, и ее к МПД алгоритмам. Но эта очевидная истина была сразу и полностью принята научной школой ОТ еще в годы физтеховской юности этой школы под руководством ныне профессора ИКИ РАН В.В. Золотарева. Так что все последующие достижения школы в области ОТ – новые коды, быстрые алгоритмы декодирования и методы настройки элементов декодеров – были получены именно множеством оптимизационных технологий [9, 10], которые в эксперименте выдавали параметры алгоритмов практически «мгновенно». А у теоретиков так ничего и не появилось. Ведь оптимизационный эксперимент – это всегда большие работы по программированию.

Таким образом, празднующее свой юбилей а.с. В.В. Золотарева уже просто фактом своего появления и главными свойствами перевело прежнюю ТК в режим быстрой отмены, так как никаких алгоритмов, кроме давних алгебраических со слабыми характеристиками так у «той» ТК и не появилось. А если формул для итоговых характеристики нет, то единственный метод, доступный всем в этом случае – моделирование алгоритмов, например, на компьютере. И это всегда программирование или, как в случае технологий ОТ, использование всех программных ресурсов почти сотни типов, которые регулярно выкладывает научная школа ОТ с инструкциями по их применению.

Таким образом, совершенно различная эффективность двух теорий очень наглядно показала, что основная задача ТК – вовсе не математическая задача, а типичная сложная вычислительная оптимизационная проблема в дискретных пространствах, крайне сложных для анализа структурах. В реальности столь сложные задачи никогда не имеют итоговых формульных решений. Но, например, в случае с ОТ, практически всегда разработчики алгоритмов декодирования со всеми реальными типами сигналов имеют хорошую поддержку в своих исследованиях в виде различных границ для значений важнейших параметров. Это хорошо помогает быстро оценивать реалистичность предлагаемых новых алгоритмов и проводить различные усовершенствования разрабатываемых методов.

Но уже пора обратиться и к третьему юбилейному для новой теории ОТ обстоятельству. В этом году исполняется 40 лет с момента полного завершения разработки ОТ как всеобщей прикладной теории создания алгоритмов коррекции ошибок с линейной сложностью и с наилучшей оптимальной достоверностью декодирования используемых эффективных длинных кодов. А итоговым заветным «золотым кирпичом» в стройном здании новой теории помехоустойчивого кодирования оказались декодеры для двоичных кодов.

Да, в ОТ создали специальные мажоритарные алгоритмы для недвоичных кодов, чего раньше ни в каком приемлемом для инженеров виде не было. Они были названы символьными и, как все прочие декодеры в ОТ, имели линейную сложность и сходились к ОТ. Этот, несомненно, великий праздник новой теории пришел к школе ОТ 40 лет назад с публикаций в 1984 г. [11] в отраслевом журнале всех основных свойств новых символьных кодов и декодеров, а в 1985 г. эти результаты уже были предъявлены в расширенном виде в престижном академическом издании [12]. И это был последний тип моделей классических для ТК каналов, рассмотренных в ОТ, чем и была действительно полностью завершена во всех своих базовых формах ОТ – новая ТК. Все алгоритмы в ОТ теперь имели линейную сложность и быстро сходились к решению ОД.

И в связи с этим стоит еще раз подчеркнуть, что школа ОТ в лучших традициях популяризации знаний в нашей науке сразу опубликовала все сведения об использованном программном обеспечении, представило макеты программ декодирования и даже предложила некоторые коды, которые могут быть применены в символьных МПД. Однако теоретики, как сторонники «той» школы, и в этом случае, не получив никаких собственных аналитических подтверждений характеристикам МПД для недвоичных кодов, не приняли новые методы кодирования, созданные, как и остальной софт в ОТ, на базе оптимизационных алгоритмов. Но время все расставило по полочкам, и даже сейчас, через 40 лет после первых статей по символьным МПД, никакие исследовательские группы мира не представили ни одной работы, в которых были бы описаны хоть какие-то коды, лучшие, чем коды РС, не говоря уже об уровне возможностей кодирования символьных кодов в ОТ.

Завершая наши заметки о каскаде юбилеев в исключительно плодотворной технологичной теории ОТ российских ученых, действительно решивших грандиозную по своим масштабам проблему цифрового мира, поставленную Шенноном, укажем, что роль школы ОТ в современной ТК, созданной исключительно ими и с детальной проработкой, во всех своих важнейших аспектах, на самом деле оказывается еще гораздо более широкой и ценной.

Пожелаем небольшой высокопрофессиональной школе ОТ, решившей 40 лет назад сложнейшую задачу, поставленную великим Шенноном, и после уже упомянутых трех юбилеев продолжать научную, образовательную и популяризаторскую деятельность в области «цифры» на своих четырех сетевых порталах www.mtdbest.ru, www.decoders-zolotarev.ru, www.decmtdzol.ru и www.mtdbest.iki.rssi.ru, которые ежегодно просматривают до 100 тыс. специалистов из более 80 стран мира.

Библиографический список

1. **Shannon C.E.** A Mathematical Theory of Communication // Bell System Technical Journal. 1948. Т. 27. С. 379-423, 623-656.
2. **Hamming R.W.** Error detecting and error correcting codes // Bell System Tech. Journal. 1950. No. 29. P. 147-160.
3. **Peterson W.W.** Error-Correcting Codes. M.I.T. Press. 1961.
4. **Reed I.S., Solomon G.** Polynomial Codes over Certain Finite Fields // Journal of the Society for Industrial and Applied Mathematics. 1960. 8 (2). P. 300-304.
5. **Viterbi A.J.** Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm // IEEE Transactions on Information Theory. 1967. Volume IT-13. P. 260-269.
6. **Золотарев В.В.** Устройство для декодирования линейных кодов. а.с. СССР № 492878.
7. **Massey J.L.** Threshold Decoding. M.I.T. Press. 1963.
8. **Самойленко С.И., Давыдов А.А., Золотарёв В.В., Третьякова Е.Л.** Вычислительные сети. М.: Наука. 1981. 278 с.
9. **Zolotarev V., Zubarev Y., Ovechkin G.** Optimization Coding Theory and Multithreshold Algorithms. Geneva, ITU. 2015, 159 p. (e-book reference: <http://www.itu.int/pub/S-GEN-OCTMA-2015>).
10. **Золотарев В.В.** Теория кодирования как задача поиска глобального экстремума (Оптимизационная теория помехоустойчивого кодирования – новая «квантовая механика» теории информации). Под научной редакцией академика РАН Н.А. Кузнецова. М.: Горячая линия – Телеком. 2018, 220 с.

11. **Золотарев В.В.** Многопороговое декодирование в недвоичных каналах // Вопросы радиоэлектроники, серия ЭВТ. 1984. Вып.12. С. 73-76.

12. **Золотарев В.В.** Алгоритмы коррекции символьных данных в вычислительных сетях // В сб.: «Вопросы кибернетики», ВК-105, АН СССР. Научный совет по комплексной проблеме «Кибернетика». М. 1985. С.54-62.

UDC 519.72

ON THREE SIGNIFICANT ANNIVERSARIES OF CODING THEORY

G. V. Ovechkin, Dr. Sc. (Tech.), associate professor, Head of Computational and Applied Mathematics Department, RSREU, Ryazan, Russia;

orcid.org/0000-0001-6887-2217, e-mail: g_ovechkin@mail.ru

A. N. Pylkin, Dr. Sc. (Tech.), associate professor, Professor of Computational and Applied Mathematics Department, RSREU, Ryazan, Russia;

orcid.org/0000-0001-9925-2870, e-mail: pylkin.a.n@rsreu.ru

*The problem of error correction when transmitting data over noisy channels, the effective solution of which is based on the use of error-correction codes and methods for their decoding is considered. **The aim of the work** is to familiarize the reader with the main stages of coding theory development. The most significant results, the appearance of which led to the emergence and development of both classical coding theory and optimization coding theory are described.*

Keywords: coding theory, optimization coding theory, error-correcting codes, binary codes, symbolic codes, error propagation, multi-threshold decoding algorithm.

DOI: 10.21667/1995-4565-2024-90-153-157

References

1. **Shannon C.E.** A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948. Vol. 27, pp. 379-423, 623-656.

2. **Hamming R.W.** Error detecting and error correcting codes // *Bell System Tech. Journal*. 1950, no. 29, pp.147-160.

3. **Peterson W.W.** *Error-Correcting Codes*, M.I.T. Press. 1961.

4. **Reed I.S., Solomon G.** Polynomial Codes over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics*. 1960, 8 (2), pp. 300-304.

5. **Viterbi A.J.** Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm. *IEEE Transactions on Information Theory*. 1967, vol. IT-13, pp. 260-269.

6. **Zolotarev V.V.** *Ustroystvo dlya dekodirovaniya lineynykh kodov*. a.s. SSSR № 492878.

7. **Massey J.L.** *Threshold Decoding*. M.I.T. Press. 1963.

8. **Samoylenko S.I., Davydov A.A., Zolotarov V.V., Tret'yakova Ye.L.** *Vychislitel'nyye seti*. Moscow: Nauka. 1981, 278 p. (in Russian).

9. **Zolotarev V., Zubarev Y., Ovechkin G.** *Optimization Coding Theory and Multithreshold Algorithms*. Geneva, ITU. 2015, 159 p. (e-book reference: <http://www.itu.int/pub/S-GEN-OCTMA-2015>).

10. **Zolotaryov V.V.** *Teoriya kodirovaniya kak zadacha poiska global'nogo ekstremuma* / Pod nauchnoj red. akademika RAN N.A. Kuznecova. Moscow: Goryachaya liniya-Telekom. 2018. 220 p. (in Russian).

11. **Zolotarev V.V.** Mnogoporogovoye dekodirovaniye v nedvoichnykh kanalach. *Voprosy radioelektroniki, seriya EVT*. 1984, no.12, pp. 73-76. (in Russian).

12. **Zolotarev V.V.** Algoritmy korrektsii simvol'nykh dannyykh v vychislitel'nykh setyakh. V sb.: *Voprosy kibernetiki*, ВК-105, АН СССР, Nauchnyy sovet po kompleksnoy probleme «Kibernetika». Moscow. 1985, pp. 54-62. (in Russian).