# АЛГОРИТМ УСКОРЕНИЯ РАБОТЫ НЕДВОИЧНОГО МНОГОПОРОГОВОГО ДЕКОДЕРА

доц. Овечкин Г.В.[1], доц. Овечкин П.В.[1], доц. Сатыбалдина Д.Ж.[2], доц. Ташатов Н.Н.[2]

[1] Рязанский государственный радиотехнический университет (РГРТУ)
[2]Евразийский национальный университет им. Л.Н. Гумилева (ЕНУ)

## Введение

Помехоустойчивое кодирование используется для исправления ошибок, возникающих при передаче данных по каналам с шумами. Основное внимание в литературе уделяется двоичным помехоустойчивым кодам, работающим с данными на уровне отдельных битов. Однако во многих цифровых системах часто удобнее работать с данными, имеющими байтовую структуру. Например, удобнее работать с байтами в системах хранения больших объемов информации (оптические диски и др. носители). В подобных системах для защиты данных от ошибок целесообразно применение недвоичных помехоустойчивых кодов. В настоящее время наиболее широкое применение среди недвоичных кодов нашли коды Рида-Соломона (РС), для которых существуют алгебраические алгоритмы декодирования [1], позволяющие исправлять до половины кодового расстояния ошибок, а также более сложные алгоритмы [2], обеспечивающие исправление большего числа ошибок. Однако данные методы из-за высокой сложности реализации позволяют декодировать только короткие и поэтому малоэффективные РС коды. В последнее время многие специалисты занимаются развитием декодеров недвоичных низкоплотностных кодов ($q$LDPC), которые способны обеспечить очень высокую эффективность [3, 4]. Однако сложность таких декодеров, особенно при большом размере символа, все еще остается слишком высокой для практического применения.

Особое место среди недвоичных алгоритмов коррекции ошибок занимают рассматриваемые далее недвоичные самоортогональные коды и соответствующие им специальные высокоскоростные символьные многопороговые декодеры ($q$МПД) [5…7], являющиеся развитием двоичных многопороговых декодеров (МПД) [7]. Представленные в [5, 6] результаты исследований показывают, что $q$МПД существенно перекрывают по своей эффективности РС коды и практически реализуемые $q$LDPC коды, оставаясь столь же простыми в реализации, как и их прототипы – двоичные МПД**.** Большую роль играет и отсутствие необходимости использования умножений в недвоичных полях при кодировании и декодировании, а также полная независимость длин символьных кодов от размеров используемых символов. Поэтому такие коды обязательно найдут широкое применение в сфере обработки, хранения и передачи больших объемов аудио- , видео- и других типов данных. Рассмотрим их более подробно.

## Недвоичные многопороговые декодеры

Опишем принципы работы $q$МПД при декодировании недвоичных самоортогональных кодов ($q$СОК). Описание дано для $q$-ичного симметричного канала ($q$СК) с размером алфавита $q$, $q > 2$, и вероятностью искажения символов $p_0$.

Пусть задан линейный недвоичный систематический сверточный или блоковый самоортогональный код, проверочная матрица **H** которого имеет такой же вид, как и в двоичном случае [7], т.е. состоит только из нулей и единиц, за исключением того, что вместо 1 в единичной подматрице будут –1, т.е. $\mathbf{H} = [\mathbf{P} : -\mathbf{I}]$. Здесь **P –** подматрица, определяемая порождающим полиномом для $q$СОК; **I** – единичная подматрица. Порождающая матрица такого кода будет иметь вид $\mathbf{G} = [\mathbf{I} : \mathbf{P}^{\mathrm{T}}]$. Данный код может использоваться при любом размере алфавита $q$. Отметим, что для заданного таким образом $q$СОК при выполнении кодирования и декодирования требуются только операции сложения и вычитания по модулю $q$. Вычисления в недвоичных полях в данном случае не используются.

Пример схемы, реализующей операцию кодирования блоковым $q$СОК, заданного полиномом $g(x) = 1+x+x^4+x^6$, представлен на рис. 1. Такой код характеризуется параметрами: длина кода $n$=26 символов, длина информационной части кода $k$=13 символов, кодовая скорость $R$=1/2, кодовое расстояние $d$=5.

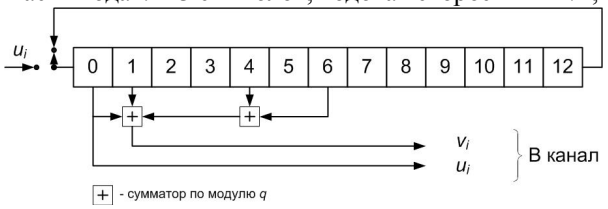


Рис. 1. Кодер для блокового $q$СОК, заданного полиномом $g(x) = 1+x+x^4+x^6$

Пусть кодер выполнил кодирование информационного вектора $\boldsymbol{U}$ и получил кодовый вектор $\boldsymbol{A}=[\boldsymbol{U},\boldsymbol{V}]$, где $\boldsymbol{V}=\boldsymbol{U}\cdot\mathbf{G}$. Отметим, что здесь и далее при выполнении операций умножения, сложения и вычитания

векторов и матриц используется модульная арифметика. После передачи кодового вектора $\boldsymbol{A}$ длины $n$ с $k$ информационными символами по $q$СК в декодер поступает вектор $\boldsymbol{Q}$, возможно, отличающийся от исходного кодового вектора из-за искажений в канале: $\boldsymbol{Q}=\boldsymbol{A}+\boldsymbol{E}$, где $\boldsymbol{E}$ – вектор шума канала типа $q$СК.

Алгоритм работы $q$МПД при декодировании вектора $\boldsymbol{Q}$ заключается в следующем [6, 7].

1. Вычисляется вектор синдрома $\boldsymbol{S}=\mathbf{H}\cdot\boldsymbol{Q}^{\mathrm{T}}$. Обнуляется разностный регистр $\boldsymbol{D}$. В данном регистре будут отмечаться измененные декодером информационные символы. Отметим, что число ненулевых элементов векторов $\boldsymbol{D}$ и $\boldsymbol{S}$ всегда будет определять расстояние между принятым из канала сообщением $\boldsymbol{Q}$ и кодовым словом, являющимся текущим решением $q$МПД. И задачей декодера является найти такое кодовое слово, для которого число ненулевых элементов векторов $\boldsymbol{D}$ и $\boldsymbol{S}$ будет минимальным. Данный шаг полностью соответствует двоичному случаю.

2. Для произвольно взятого $q$-ичного декодируемого информационного символа $i_j$ принятого сообщения подсчитывается число двух наиболее часто встречающихся значений проверок $s_j$ вектора синдрома $\boldsymbol{S}$ из общего числа всех проверок, относящихся к символу $i_j$, а также символа $d_j$ вектора $\boldsymbol{D}$, соответствующего символу $i_j$. Пусть значения этих двух проверок равны $h_0$ и $h_1$, а их количество равно $m_0$ и $m_1$ соответственно, причем $m_0 \geq m_1$. Данный шаг является аналогом процедуры получения суммы на пороговом элементе в двоичном МПД,

3. Если $m_0–m_1 > T$, где $T$ – значение порога (некоторое целое неотрицательное число), то из $i_j$, $d_j$ и всех проверок относительно $i_j$ вычитается оценка ошибки, равная $h_0$. Данный шаг является аналогом сравнения суммы с порогом в двоичном декодере и изменения декодируемого символа и коррекции через обратную связь всех символов синдрома, являющихся проверками для декодируемого символа.

4. Происходит выбор нового $i_m$, $m \neq j$, и осуществляется переход к п. 2.

Такие попытки декодирования по пп. 2…4 могут быть повторены для каждого символа принятого сообщения несколько раз [6, 7]. Заметим, что при реализации алгоритма $q$МПД, как и в двоичном случае, удобно все информационные символы перебирать последовательно, а останавливать процедуру декодирования после фиксированного числа попыток (итераций) коррекции ошибок или если при очередной такой итерации ни один из символов не изменил своего значения. Пример схемной реализации $q$МПД для кодера с рис. 1 представлен на рис. 2.

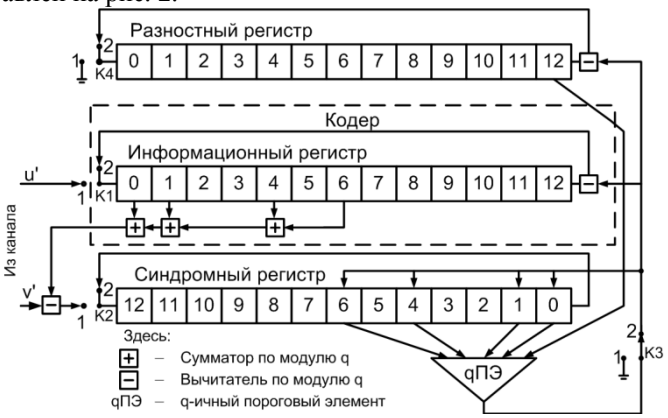


Рис. 2. $q$МПД для блокового $q$СОК

Для описанного алгоритма $q$МПД справедлива следующая теорема.

**Теорема**. Пусть декодер реализует алгоритм $q$МПД для описанного выше кода. Тогда при каждом изменении декодируемых символов происходит переход к более правдоподобному решению по сравнению с предыдущими решениями декодера.

**Доказательство теоремы** дано в [6, 7]. При доказательстве показывается, что суммарный вес Хемминга синдромного и разностного регистров при изменении декодируемого символа в соответствии с вышеописанным алгоритмом $q$МПД строго уменьшается.

Отметим наиболее существенные моменты, характеризующие предложенный алгоритм. Во-первых, как и в случае двоичных кодов, нельзя утверждать, что улучшение решения $q$МПД при многократных попытках декодирования будет иметь место до тех пор, пока не будет достигнуто решение оптимального декодера. На самом деле и в блоковых, и в сверточных кодах возможны конфигурации ошибок, не исправляемые в $q$МПД, но которые могут быть исправлены в оптимальном декодере. Поэтому основной способ повышения эффективности $q$МПД состоит в поиске кодов, в которых такие неисправляемые конфигурации ошибок довольно редки даже при большом уровне шума. Вопросы выбора таких кодов подробно рассмотрены в [7].

Другим важнейшим моментом является то, что по сравнению с традиционным подходом к мажоритарным схемам, в $q$МПД для изменения декодируемого символа достаточно наличие не абсолютного, а только относительно строгого большинства проверок, как это следует из условия $m_0–m_1 > T$. Например, в $q$СОК с $d = 9$ ошибка в декодируемом символе будет исправлена даже в том случае, если из девяти его

проверок (включая и символ $d_j$ разностного регистра) правильными будут только две, а остальные семь – ошибочными! Этого невозможно представить для двоичных кодов, а для $q$МПД такая ситуация типична.

Следует отметить, что при правильном выборе кодов $q$МПД оказывается способен обеспечить их близкое к оптимальному декодирование всего лишь с линейной сложностью реализации. В результате его характеристики помехоустойчивости оказываются много лучше, чем характеристики даже многократно более сложных декодеров для РС кодов и практически реализуемых недвоичных LDPC кодов. Например, в [8] показано, что с помощью достаточно простых каскадных кодов со скоростью 1/2, при декодировании которых используется $q$МПД, можно обеспечить вероятность ошибки декодирования порядка $10^{-9}$ при 27% байтовых ошибок в канале, что является в настоящее время недостижимым для других методов коррекции ошибок в символьных данных. Высокую эффективность $q$МПД обеспечивает и при декодировании малоизбыточных самоортогональных кодов.

**Алгоритм ускорения работы порогового элемента недвоичного многопорогового декодера**

Для решения задач безошибочной передачи и надежного хранения больших объемов данных к методам коррекции ошибок предъявляются очень жесткие требования по скорости кодирования и декодирования информации. Поэтому несмотря на то, что скорость работы $q$МПД во много раз превосходит скорость работы других недвоичных декодеров, существует возможность дополнительного ускорения работы $q$МПД. При анализе схемы недвоичного МПД, представленной на рис. 2, было показано, что $q$МПД является устройством, состоящим только из регистров сдвига, сумматоров, вычитателей по модулю $q$ и недвоичного порогового элемента. Среди этих элементов декодера наибольшую сложность имеет его пороговый элемент. Поэтому, для того чтобы ускорить $q$МПД, необходимо ускорить работу $q$ПЭ.

В процессе исследования работы $q$МПД было замечено, что часто на соседних итерациях декодирования для одного информационного символа не меняется информация, поступающая на пороговый элемент. Поэтому предлагается так модифицировать работу $q$ПЭ, чтобы в процессе декодирования по возможности использовались значения, рассчитанные пороговыми элементами предшествующих итераций, и только в случае необходимости осуществлялся их пересчет. На основании данной идеи была разработана схема модифицированного $q$МПД, представленная на рис. 3.

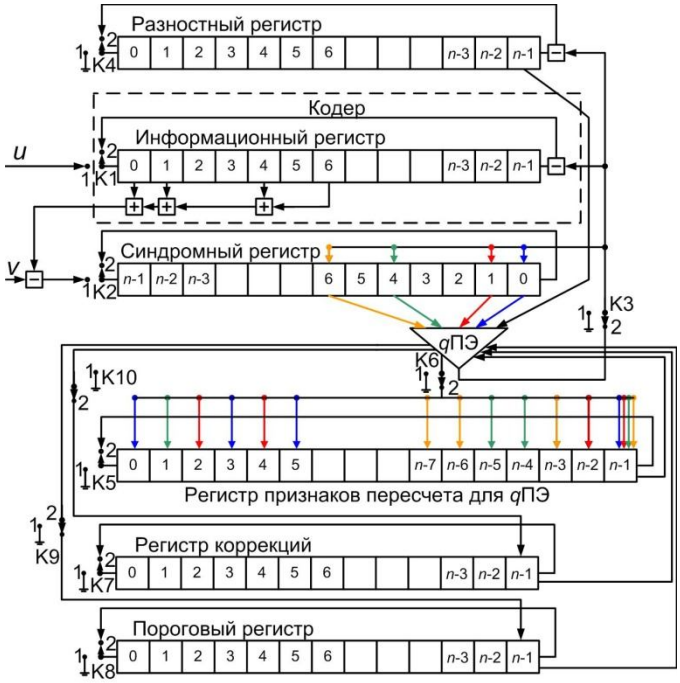


Рис.3. Модифицированный $q$МПД блокового недвоичного СОК с $R$=1/2, $d$=5

Отметим, что в эту схему вводится дополнительный регистр, элементы которого показывают, нужно ли заново обрабатывать информацию, поступающую на пороговый элемент с синдромного и разностного регистров. При этом, так как на различных итерациях может измениться значение порога $q$ПЭ, то необходимо запоминать значение разности $m_0$–$m_1$ и значение коррекции $h_0$, которое используется при срабатывании порогового элемента.

Каждый элемент регистра признаков пересчета может содержать всего два значения: 0 или 1. На первой итерации декодирования регистр признаков пересчета заполняется единицами.

Процедура декодирования принятого сообщения модифицированным $q$МПД состоит в следующем:

1. Произвольно выбирается декодируемый информационный символ $i_j$ принятого сообщения.

2. Если элемент регистра признаков пересчета, соответствующий информационному символу $i_j$, равен 1, то подсчитывается число двух наиболее часто встречающихся проверок. Значения этих двух проверок равны $h_0$ и $h_1$, а их количество равно $m_0$ и $m_1$ соответственно, причем $m_0 \geq m_1$. Если элемент регистра признаков пересчета равен 0, то значение разности $m_0 - m_1$ устанавливается равным значению текущего элемента порогового регистра, а значение $h_0$ – значению текущего элемента регистра коррекций.

3. Если $m_0 - m_1 \leq T$, то устанавливается в 0 значение элемента регистра признаков пересчета, соответствующего информационному символу $i_j$, в текущий элемент порогового регистра заносится разность $m_0 - m_1$, в текущий элемент регистра коррекций – значение $h_0$. Если $m_0 - m_1 > T$, то из $i_j$, $d_j$ и всех проверок относительно $i_j$ вычитается оценка ошибки, равная $h_0$. Также устанавливаются в 1 все элементы регистра признаков, соответствующие информационные символы которых участвовали в формировании измененных символов синдромного регистра.

4. Осуществляется переход к новому произвольному $i_m$, $m \neq j$ и далее переход к пункту 2.

В пункте 3 потребуется всего порядка $(d-1)^2 \cdot nk/nr$ изменений элементов регистра признаков пересчета в случае коррекции каждого информационного символа, где $nk$ и $nr$ – число информационных и проверочных ветвей кодера соответственно.

В табл. 1 приведены результаты сравнения времени декодирования информации обычным и модифицированным $q$МПД. Для декодирования использовался $q$СОК с $R$=7/8 и $d$=7, вероятности ошибок в канале составляли $P_0$=0.04 и $P_0$=0.001. Объем информации для декодирования $10^8$ байтовых символов.

Табл. 1 Время декодирования информации $q$МПД

| Вероятность ошибки в канале | $q$МПД | Модификация $q$МПД |
|---|---|---|
| $P_0$=0.04 | 16 минут | 8 минут |
| $P_0$=0.001 | 15 минут | 5 минут |

В результате применения модифицированного алгоритма работы $q$ПЭ быстродействие $q$МПД увеличилось в 2 раза при $P_0$=0.04 и в 3 раза при $P_0$=0.001. Отметим, что при использовании данной модификации $q$ПЭ эффективность декодирования по сравнению с обычным $q$ПЭ не снижается. Заметим, что для большего выигрыша по объему операций данную модификацию $q$МПД в некоторых случаях следует применять после нескольких обычных итераций декодирования.

## Заключение

Приведенные результаты позволяют считать, что $q$МПД методы действительно относятся к уникальным алгоритмам, способным обеспечивать эффективное декодирование при большом уровне шума, выполняя очень небольшое число операций и достигая высочайших уровней достоверности передачи и хранения цифровой информации и скорости ее обработки в высокоскоростных линиях связи и в устройствах хранения больших объемов данных.

Получены важные результаты по модификации $q$ПЭ, позволившие увеличить скорость работы $q$МПД в несколько раз. Использование такого $q$МПД для исправления ошибок в системах памяти с байтовой структурой данных может многократно повысить скорость работы программных версий алгоритмов кодирования и декодирования при реализации специальных версий декодеров с быстрыми пороговыми элементами.

Работа выполнена при финансовой поддержке РФФИ, РГРТУ и Комитета науки МОН Республики Казахстан. Большой объем дополнительной информации о МПД можно найти на веб-сайтах [9].

## Литература

1. Berlekamp E. R. Algebraic Coding Theory, McGraw-Hill, New York, 1968.
2. Wu C. New list decoding algorithms for Reed-Solomon and BCH codes IEEE Transactions on Information Theory, vol. 54, pp. 3611–3630. August 2008.
3. Declercq D., Fossorier M. Extended minsum algorithm for decoding LDPC codes over GF(q) // IEEE International Symp. on Inf. Theory, 2005, pp.464–468.
4. Zhang F., Pfister H. List-Message Passing Achieves Capacity on the q-ary Symmetric Channel for Large q // In Proc. IEEE Global Telecom. Conf., Washington, DC, Nov. 2007. pp.283–287.
5. Кузнецов Н.А., Золотарёв В.В., Овечкин Г.В., Овечкин П.В. Недвоичные многопороговые декодеры и другие методы коррекции ошибок в символьной информации // Радиотехника. – М., 2010. №6. – вып. 141. – С.4–9.
6. Золотарёв В.В., Овечкин Г.В. Эффективное многопороговое декодирование недвоичных кодов // Радиотехника и электроника. – М., 2010. Т.55. – №3. – С.324–329.
7. Золотарев В.В., Зубарев Ю.Б., Овечкин Г.В. Многопороговые декодеры и оптимизационная теория кодирования. М.: Горячая линия – Телеком, 2012. 239 с.
8. Овечкин Г.В., Овечкин П.В. Оптимизация структуры недвоичных самоортогональных кодов для схем параллельного кодирования // Труды НИИР, 2009. – №2. – С.34–38.
9. Веб-сайты ИКИ РАН www.mtdbest.iki.rssi.ru и РГРТУ www.mtdbest.ru.