

УДК 579.6

Алгоритмы декодирования кодов с низкой плотностью проверок на четность*А.Н. Гамова, К.А. Самохина**СГУ им. Н.Г. Чернышевского, г. Саратов*

С развитием телекоммуникационных технологий интерес к передаче информации с минимальным количеством ошибок снова вырос. Коды с низкой плотностью проверки на четность стали частью стандарта DVB-S2 спутниковой передачи данных для цифрового телевидения и вошли в стандарт IEEE 802.3an сети Ethernet 10G. Замена произошла и в стандарте DVB-T2 для цифрового телевизионного вещания.

Коды с низкой плотностью проверок на четность – мощная техника исправления ошибок, которая выигрывает у многих известных схем кодирования. Коды могут использоваться в любой системе связи, где существенно экономия энергии или отношение сигнал/шум очень низко.

Коды с низкой плотностью проверок на четность (LDPC) – это линейные блочные коды, проверочная матрица которых является разреженной, то есть содержит малое количество ненулевых элементов. В зависимости от вида LDPC-кода и способа его синтеза, число ненулевых элементов в проверочной матрице будет варьироваться. Помимо матричного описания, LDPC-коды также могут быть описаны с помощью двудольного неориентированного графа Таннера. Двудольным он называется, потому что узлы графа разделены на два различных множества, а ребра соединяют только узлы двух разных типов. Такое представление позволяет более наглядно описать алгоритм декодирования [1]. Граф Таннера содержит два типа узлов – проверочные (M) и переменные (N). Узлы разных типов соединяются друг с другом с помощью путей. Число переменных узлов соответствует числу битов в кодовом слове, т.е. числу столбцов в проверочной матрице, а число проверочных узлов соответствует числу проверочных уравнений, т.е. числу строк в проверочной матрице. Переменный узел n соединяется с проверочным узлом m только в том случае, если в проверочной матрице в столбце n и в строке m находится единица. Степень узла показывает число ребер, выходящих из данного узла. В графе Таннера могут возникать циклы, которых нужно избегать, для получения оптимальных результатов при кодировании и декодировании данного кода. Цикл представляет собой после-

довательность подключенных узлов, которые начинаются и заканчиваются в одном и том же узле на графе, который содержит более одного ребра. Длина цикла – это количество содержащихся в нем ребер, а обхват графа – это размер его наименьшего цикла. Двоичный линейный (n, k) – код, заданный проверочной матрицей H , называется (J, K) регулярным кодом с малой плотностью проверок на четность, если каждый столбец матрицы H содержит ровно J единиц, а каждая строка K единиц. Подразумевается, что числа J и K малы по сравнению с длиной и размерностью кода. Если рассматривается последовательность кодов с фиксированной скоростью $R = k/n$ и с возрастающей длиной n и размерностью k , то параметры J и K остаются неизменными. В исследованиях последних лет много внимания уделяется иррегулярным LDPC-кодам, фиксирующих не вес столбцов и строк, а наборы весов с предопределенными вероятностями. Одной из распространенных конструкций для LDPC-кодов является метод, предложенный Маккеем и Нилом. В этом методе столбцы H добавляются по одному столбцу слева направо. Вес каждого столбца выбирается таким образом, чтобы получить правильное распределение бит и расположение ненулевых элементов в каждом столбце, выбираемых случайным образом из тех строк, которые еще не полностью заполнены. Если в любой момент есть строки с большим количеством незаполненных позиций, тогда заполняются оставшиеся столбцы. Процесс может быть запущен снова, пока не будет получено необходимое распределение бит в строках. Поскольку в построении LDPC-кодов используются псевдослучайные методы, то можно говорить о наборе всех возможных кодов с определенными параметрами, а не о конкретном выборе проверочной матрицы с этими параметрами.

Большой проблемой случайной конструкции проверочной матрицы является кодирование, так как при большой размерности H очень сложно решить уравнение $GH^T = 0$. Но можно использовать коды повторного накопления [2]. RA-LDPC код делает кодирование очень быстрым без тяжелых вычислений. Матрица H для кода повторного накопления представляет собой композицию двух подматриц – H_s и H_p . H_s – основная подматрица H , которая контролирует информационные биты s кода c . H_p – подматрица, которая управляет битами четности p кода c . Эта подматрица размерности $m \times m$ с единицами на главной диагонали и единицами на диагонали сразу ниже главной.

Классы алгоритмов, используемых для декодирования LDPC-кодов, в совокупности называются алгоритмами передачи сообщений, поскольку их работа может быть объяснена передачей сообщения по вершинам графа Таннера. Каждый узел работает изолированно, имея доступ только к сообщениям на вершинах, связанных с ним. Итеративный

алгоритм декодирования – это алгоритм, где сообщения передаются между переменными и проверочными узлами итеративно, пока результат не будет достигнут (или процесс будет остановлен). В основе работы данных методов лежит обмен мягкими решениями по итерациям между переменными и проверочными узлами графа кода. В случае, если на графе отсутствуют циклы, применение такого способа декодирования позволяет получить оптимальное решение [3]. К данным методам относятся такие алгоритмы, как алгоритм инверсии битов (BF), алгоритм суммарного произведения (SPA) и алгоритм минимальной суммы (MS). Алгоритм суммарного произведения, основанный на вероятностях, близок к алгоритму инверсии битов, но сообщения, представляющие каждое решение (независимо от того, является ли значение бита 1 или 0), теперь являются вероятностными. В то время как декодирование с инверсией битов принимает исходное жесткое решение по принимаемым битам на входе, алгоритм суммарного произведения представляет собой алгоритм с мягким выбором, который принимает в качестве входного сигнала вероятность для каждого принятого бита. Принятые вероятности битов также называют априорными вероятностями для принятых битов, поскольку они были известны заранее, прежде чем начал работать LDPC декодер.

Одним из преимуществ LDPC-кодов в сравнении с другими видами кодирования является эффективный алгоритм декодирования с линейной сложностью от длины кодового слова – алгоритм с итеративным распространением доверия. Существует три разновидности этого алгоритма: основанный на вероятностях (SPA-Prob), на логарифмическом отношении функций правдоподобия (SPA-LLR) и с жестким решением (SPA-Hard).

Результаты моделирования алгоритмов. Для анализа алгоритмов был выбран метод зависимости вероятности ошибки на бит (BER) от соотношения сигнал/шум (SNR). Программа написана на языке программирования Matlab в среде разработки Matlab R2017b, где было получено большое число графиков и диаграмм, характеризующих эффективность работы декодеров.

а) Сравнивалась эффективность исправления ошибок алгоритмов инверсии битов и минимальной суммы в зависимости от количества итераций, скорости построения кода, метода конструкции проверочной матрицы.

б) Описывалась зависимость эффективности алгоритмов суммарного произведения от метода конструкции проверочной матрицы и длины кодового слова.

с) Выяснялось, какой из алгоритмов с жестким решением лучше использовать в той или иной ситуации.

д) Проводилось сравнение эффективности исправления ошибок всех рассмотренных алгоритмов.

По полученным результатам сделаны следующие выводы и рекомендации к применению:

1) при изменении метода декодирования можно уменьшить вероятность ошибки в символе, при увеличении количества итераций вероятность ошибки также уменьшалась;

2) алгоритмы SPA-LLR и SPA-Prob давали самые лучшие результаты;

3) SPA-LLR и SPA-Prob имеют одинаковую вероятность ошибки, но первый выигрывает по времени;

4) разновидности алгоритмов суммарного произведения показывают лучшие результаты на кодах со случайной проверочной матрицей;

5) все алгоритмы работают эффективнее на кодовых словах с большой длиной;

6) алгоритм MS дает результат чуть хуже SPA-LLR и SPA-Prob, но значительно выигрывает по времени;

7) если выбирать из алгоритмов с жестким решением, то при малых значениях отношения сигнал/шум лучше использовать SPA-Hard.

8) алгоритмы с жестким решением работают быстрее, чем с мягким.

Библиографический список

1. Кравченко А. Н. Снижение сложности декодирования низкоплотного кода. // Цифровая обработка сигналов – М., 2010. – №2. – С. 35–41.

2. Кравченко А.Н. Методы и аппаратура кодирования и декодирования систематического нерегулярного кода повторения-накопления (IRA) для DVBS2 и DVB-T2 демодуляторов [Электронный ресурс] // Цифровая обработка сигналов, 2009. Вып. 4.

3. Акулинин С. А. Выбор параметров LDPC-кодов для каналов с аддитивным белым гауссовским шумом. [Электронный ресурс] // Вестник Воронежского государственного университета, 2015. Вып. № 4.