МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

Коды с низкой плотностью проверок на четность

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Самохиной Ксении Алексеевны

Научный руководитель
к. ф.-м. н, доцент _____ А. Н. Гамова
18.01.2019 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
18.01.2019 г.

Саратов 2019

ВВЕДЕНИЕ

В настоящее время получили широкое распространение и продолжают быстро развиваться области, связанные с обработкой и передачей данных – локальные проводные сети, мобильная связь, беспроводные сети, устройства хранения данных. Важной задачей является повышение эффективности существующих методов передачи. Коды с низкой плотностью проверок на четность (LDPC-коды) на данный момент являются наиболее эффективными. С развитием телекоммуникационных технологий интерес к передачи информации с минимальным количеством ошибок вырос. Эти коды 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 [6].

Целью дипломной работы является изучение кодов с низкой плотностью проверок на четность, рассмотрение способов описания и построения этих кодов, кодирования. Необходимо изучить алгоритмы декодирования, такие как алгоритм инверсии битов, алгоритм суммарного произведения и алгоритм минимальной суммы. Затем реализовать алгоритмы декодирования и сравнить их на эффективность и работоспособность. Код с низкой плотностью проверок на чётность – мощная техника исправления ошибок, которая выигрывает у многих известных схем кодирования. Код может использоваться в любой системе связи, где существенна экономия энергии.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 62 страницы, из них 45 страниц – основное содержание, включая 32 рисунка и 1 таблицу, список использованных источников из 21 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе описывается актуальность кодов с низкой плотностью проверок на четность и где они используются.

Во втором разделе приведены необходимые определения. Отличительной чертой LDPC-кодов от классических линейных блоковых кодов является то, что при кодировании и декодировании LDPC-кодов не используется порождающая матрица кода. Вместо порождающей матрицы для описания кодирования и декодирования LDPC-кодов используется проверочная матрица кода.

Коды с низкой плотностью проверок на четность – это линейные блоковые коды, проверочная матрица которых является разреженной, то есть содержит малое количество ненулевых элементов. Точного критерия, согласно которому матрица считается разреженной, не существует. В зависимости от вида LDPC-кода и способа его синтеза, число ненулевых элементов в проверочной матрице будет варьироваться [9].

В первом подразделе описываются способы, с помощью которых можно представить код, матричный и граф Таннера. Граф Таннера содержит два типа узлов – проверочные и переменные. 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 [10].

Во втором подразделе рассматриваются два способа конструкции кода: случайный и алгебраический. Случайный, в свою очередь, делится на регулярный и иррегулярный. Двоичный линейный код (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. Иррегулярный LDPC-код фиксирует не вес столбцов и строк, а наборы весов, из которых разрешено выбирать значения в соответствии с некоторыми предопределенными вероятностями [12]. Алгебраический способ основан на матрицах перестановок.

Третий подраздел содержит условия, которые необходимы для создания кода LDPC с высокими характеристиками:

1. Эффективность кода возрастает, когда циклы в графе Таннера кода LDPC становятся более длинными.

2. LDPC-код обладает эффективным кодированием по сравнению со сверточным или турбо-кодом, но трудно выполнимое в режиме реального времени. Поэтому для уменьшения сложности кодирования кода LDPC был предложен код повторного накопления (repeat-accumulate, RA).

3. Если сопоставить регулярный код с иррегулярным, то второй обладает более высокими характеристиками [16].

В третьем разделе описывается кодирование. Для кодирования используется RA-LDPC код, который 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.

Кодирование является систематическим и происходит в два этапа. Полученное кодовое слово имеет первыми k информационных бит и затем m проверочных бит. Проверочные биты вычисляются по следующим формулам:

$$p_1 = \sum_{i=1}^{k} H_{s1i} s_i = v_1,$$
$$p_2 = p_1 + \sum_{i=1}^{k} H_{s2i} s_i = p_1 + v_2,$$
$$p_3 = p_2 + \sum_{i=1}^{k} H_{s3i} s_i = p_2 + v_3,$$
$$\ldots$$
$$p_m = p_{m-1} + \sum_{i=1}^{k} H_{smi} s_i = p_{m-1} + v_m.$$

Результат кодирования – кодовое слово $c = [s|p]$ [15].

Четвертый раздел содержит описание алгоритмов декодирования.

Алгоритм инверсии битов (BF):

На первом шаге алгоритма осуществляется инициализация максимального количества итераций. В случае если текущее число итераций алгоритма достигнет максимального значения и произведение декодируемого слова на проверочную матрицу не будет равно нулю, то это будет означать отказ декодирования.

На втором шаге осуществляется расчет синдрома.

На третьем шаге алгоритма формируется временная матрица путем поэлементного умножения каждого столбца проверочной матрицы на вектор синдрома. Затем строки временной матрицы суммируются и находится позиция максимального значения суммарной строки. В случае если позиций, соответствующих максимальному значению, несколько, то выбирается одна из них случайным образом. Эта позиция соответствует биту кодового слова, для которого наибольшее количество проверок на четность не было выполнено и такой бит является наиболее недостоверным. Соответствующий этой позиции кодовый бит инвертируется, и алгоритм переходит ко второму шагу. В случае если максимальное значение суммарной строки равно нулю, то это говорит об отсутствии ошибок в декодируемом кодовом слове, тогда алгоритм завершается.

На последнем шаге алгоритма осуществляется проверка текущего числа итераций. Если текущее значение равно максимальному, то алгоритм декодирования завершается отказом. В противном случае алгоритм переходит ко второму шагу.

Алгоритм суммарного произведения, основанный на вероятностях (SPA-Prob):

Шаг 1. В случае аддитивного белого гауссова шума (АБГШ) инициализировать априорные вероятности переменных узлов, равными:

$$q_{ji}(0) = 1 - P_j = \Pr\left(c_j = 0 \mid y_j\right) = \frac{1}{1+e^{-2y_j/\sigma}},$$

$$q_{ji}(1) = P_j = \Pr\left(c_j = 1 \mid y_j\right) = \frac{1}{1+e^{2y_j/\sigma}}$$

Шаг 2. Для всех i и j вычислить $r_{ij}(0)$ и $r_{ij}(1)$ в соответствии с выражениями $r_{ij}(0) = \frac{1}{2} + \frac{1}{2}\prod_{j' \in N(i)\setminus j}(1 - 2q_{j'i}(1))$ и $r_{ij}(1) = 1 - r_{ij}(0)$.

Шаг 3. Для всех i и j вычислить $q_{ij}(0)$ и $q_{ij}(1)$ в соответствии с выражениями

$$q_{ji}(0) = (1 - P_j)\prod_{i' \in M(j)\setminus i} r_{i'j}(0),$$

$$q_{ji}(1) = P_j \prod_{i' \in M(j)\setminus i} r_{i'j}(1)$$

и нормировать с множителем $k_{ij} = \frac{1}{q_{ji}(0)+q_{ji}(1)}$:

$$q_{ji}(0) = k_{ij}(1 - P_j)\prod_{i' \in M(j)\setminus i} r_{i'j}(0),$$

$$q_{ji}(1) = k_{ij}P_j \prod_{i' \in M(j)\setminus i} r_{i'j}(1).$$

Шаг 4. Для всех j вычислить апостериорные вероятности

$$Q_j(0) = (1 - P_j)\prod_{i \in M(j)} r_{ij}(0),$$

$$Q_j(1) = P_j \prod_{i \in M(j)} r_{ij}(1).$$

и нормировать множителем с $K_j = \frac{1}{Q_j(0)+Q_j(1)}$:

$$Q_j(0) = K_j(1 - P_j)\prod_{i \in M(j)} r_{ij}(0),$$

$$Q_j(1) = K_j P_j \prod_{i \in M(j)} r_{ij}(1).$$

Шаг 5. Проверить кодовое слово $\hat{c} = [\hat{c}_0, \hat{c}_1, \dots, \hat{c}_{n-1}]$, где $\hat{c}_j = 1$, если $Q_j(1) > Q_j(0)$, иначе $\hat{c}_j = 0$ на предмет принадлежности коду, то есть $\hat{c}H^T = 0$. Если это условие выполняется, то производится остановка алгоритма. Если это условие не выполняется, то возврат к шагу 2, до тех пор, пока не будет превышено некоторое предельное число итераций [9].

Алгоритм суммарного произведения, основанный на логарифмическом отношении функций правдоподобия (SPA-LLR):

Шаг 1. Для всех $j = 0, 1, \dots, n-1$ инициализировать переменные узлы равными логарифмическому отношению априорных вероятностей Q_{ji}: $Q_{ji} = l_j = 2y_j/\sigma^2$, где σ^2 – дисперсия АБГШ.

Шаг 2. Для всех i и j вычислить R_{ij} в соответствии с выражением

$$R_{ij} = 2\tanh^{-1}\Big(\prod_{j' \in N(i)\setminus j} \tanh\Big(\frac{Q_{j'i}}{2}\Big)\Big).$$

Шаг 3. Для всех j и i вычислить Q_{ji} в соответствии с выражением $Q_{ji} = l_j +$

$+ \sum_{i\prime \in M(j)\backslash i} R_{i\prime j}$.

Шаг 4. Вычислить логарифмические отношения апостериорных вероятностей в соответствии с формулой $P_j = l_j + \sum_{i \in M(j)} R_{ij}$.

Шаг 5. Проверить кодовое слово $\hat{c} = [\hat{c}_0, \hat{c}_1, \dots, \hat{c}_{n-1}]$, где $\hat{c}_j = 1$, если $P_j \leq 0$, иначе $\hat{c}_j = 0$. Если $\hat{c}H^T = 0$ или число итераций равно максимальному установленному значению, то производится остановка алгоритма, иначе переход к шагу 2 [9].

Алгоритм суммарного произведения с жестким решением (SPA-Hard):

Основная идея состоит в том, чтобы подсчитать все проверочные узлы и затем проверить узлы, которые не соответствуют условию корректности проверочного узла (что подразумевает нулевое значение), вернуть переменным узлам противоположные значения. Наиболее частое входящее значение берется за результат [21].

Алгоритм минимальной суммы (MS):

Выражение $R_{ij} = 2\tanh^{-1}(\prod_{j\prime \in N(i)\backslash j} \tanh(\frac{Q_{j\prime i}}{2}))$ может быть преобразовано следующим образом

$$R_{ij} = 2\tanh^{-1}\left(\prod_{j\prime \in N(i)Jay} \tanh\left(\frac{Q_{j\prime i}}{2}\right)\right) = \prod_{j\prime \in N(i)\backslash j} sign\left(Q_{j\prime i}\right) *$$

$$* 2\tanh^{-1}(\prod_{j\prime \in N(i)\backslash j} \tanh(|Q_{j\prime i}|/2)).$$

Алгоритм минимальной суммы упрощает вычисление R_{ij}, считая, что член, соответствующий наименьшему, стоит выше результата произведения, и поэтому внешняя информация может быть аппроксимирована минимумом:

$$R_{ij} = \prod_{j\prime \in N(i)\backslash j} sign\left(Q_{j\prime i}\right) \min_{j\prime \in N(i)\backslash j} |Q_{ji\prime}|.$$

При выполнении вертикального шага, как и при суммарном произведении, рассчитывается значение суммарного логарифмического отношения правдоподобия [9].

В пятом разделе первом подразделе описывается интерфейс реализованной программы, инструкция по использованию и примерами

работоспособности. Во втором подразделе происходит моделирование алгоритмов декодирования в зависимости от различных параметров. Для анализа алгоритмов был выбран метод зависимости вероятности ошибки на бит от соотношения сигнал/шум. Сравнивается эффективность исправления ошибок алгоритма инверсии битов и минимальной суммы в зависимости от количества итераций, скорости кода, метода конструкции проверочной матрицы. Описывается зависимость эффективности алгоритмов суммарного произведения от метода конструкции проверочной матрицы, длины кодового слова. Также происходит сравнение алгоритмов суммарного произведения между собой. В данном подразделе выясняется, какой из алгоритмов с жестким решением лучше использовать в той или иной ситуации.

Приводится сравнение эффективности исправления ошибок всех рассмотренных алгоритмов. По полученным результатам сделаны следующие выводы:

1. при изменении метода декодирования можно уменьшить вероятность ошибки в символе, при увеличении количества итераций вероятность ошибки также уменьшается;
2. алгоритмы SPA-LLR и SPA-Prob дают самые лучшие результаты;
3. SPA-LLR и SPA-Prob имеют одинаковую вероятность ошибки, но первый выигрывает по времени;
4. разновидности алгоритма 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, иначе BF;
8. алгоритмы с жестким решением работают быстрее, чем с мягким.

ЗАКЛЮЧЕНИЕ

В ходе работы были рассмотрены коды с низкой плотностью проверок на четность, способы их описания, методы построения, изучено кодирование и алгоритмы декодирования этих кодов.

При написании программы были реализованы алгоритмы случайного и алгебраического построения разреженной проверочный матрицы, алгоритм систематического кодирования, алгоритмы декодирования. При сравнении результатов работы алгоритмов были получены графики вероятности ошибки на бит для различных случаев: сравнительная работа мягкого и жесткого декодеров, влияние количества итераций на корректирующую способность декодера, влияние размера проверочной матрицы на корректирующую способность декодера, зависимость результата от метода построения проверочной матрицы. Таким образом, в ходе выполнения работы, поставленные задачи были успешно выполнены в полной мере.

На основании результатов, полученных в пятом разделе, можно выбрать алгоритм, который подходит для своих определенных целей, самый быстрый или самый эффективный по исправлению ошибок, с мягким или жестким решением.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Овчинников, А. Обработка информации при передаче LDPC-кодами по дискретным и полунепрерывным каналам [Электронный ресурс] / А. Овчинников. 2004. Загл. с экрана. Яз. рус.

2 Новиков, Р. С. Выбор параметров LDPC кодов для каналов с АБГШ [Электронный ресурс] / Р. С. Новиков, А. А. Астраханцев. Загл. с экрана. Яз. рус.

3 Лихохабин, Е. А. Исследование быстрых алгоритмов декодирования кодов с низкой плотностью проверок на четность [Электронный ресурс] / Е. А. Лихохабин // Цифровая обработка сигналов и ее применение – DSPA-2009: Труды РНТОРЭС имени А.С.Попова. Серия: Цифровая обработка сигналов и ее применения. Выпуск XI-1. – М., 2009. – С. 55-58. Загл. с экрана. Яз. рус.

4 Способ трансляции информационного телевидения [Электронный ресурс] // FindPatent.ru – патентный поиск [Электронный ресурс]. URL : http://www.findpatent.ru/patent/221/2219676.html (дата обращения 4.01.2019). Загл. с экрана. Яз. рус.

5 Галлагер, Р. Теория информации и надежная связь [Электронный ресурс] / Р. Галлагер. М. : Советское радио, 1974. Загл. с экрана. Яз. рус.

6 Золотарев, В. В. Обзор исследований и разработок методов помехоустойчивого кодирования / В. В. Золотарев, Г. В. Овечкин. Москва, 2004. – 126 с.

7 Башкиров, А. В. Основы помехоустойчивого кодирования, основные преимущества и недостатки алгоритмов декодирования [Электронный ресурс] / А. В. Башкиров, И. В. Остроумов, И. В. Свиридова // Вестник Воронежского государственного технического университета. 2012. –Т. 8. – №2. Загл. с экрана. Яз. рус.

8 Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. М. : Мир, 1986. 576 с.

9 Кравченко, А. Н. Снижение сложности декодирования низкоплотностного кода [Электронный ресурс] / А. Н. Кравченко // Цифровая обработка сигналов. 2010. Вып. №2. Загл. с экрана. Яз. рус.

10 Кравченко, А. Н. Методы и аппаратура кодирования и декодирования систематического нерегулярного кода повторения-накопления (IRA) для DVB-S2 и DVB-T2 демодуляторов [Электронный ресурс] / А. Н. Кравченко // Цифровая обработка сигналов, 2009. Вып. №4. Загл. с экрана. Яз. рус.

11 Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы алгоритмы, применение / Р. Морелос-Сарагоса : пер. с англ. В. Б. Афанасьева. М. : Техносфера, 2005. 320 с.

12 Кудряшов, Б. Д. Основы теории кодирования [Электронный ресурс] / Б. Д. Кудряшов. СПб. : БВХ-Петербург, 2016. 400 с. : ил. Загл. с экрана. Яз. рус.

13 Галлагер, Р. Дж. Коды с малой плотностью проверок на четность / Р. Дж. Галлагер : пер. с англ. А. Шевердяева. М. : Мир, 1966. 145 с.

14 Biglieri, E. Coding for wireless channels [Электронный ресурс] / E. Biglieri. Springer, 2005. Загл. с экрана. Яз. англ.

15 Johnson, S. J. Iterative error correction: turbo, low-density parity-check and repeat-accumulate codes [Электронный ресурс] / S. J. Johnson. Cambridge University Press, 2009. Загл. с экрана. Яз. англ.

16 Воробьев, К. А. Методы построения и декодирования недвоичных низкоплотностных кодов [Электронный ресурс] / К. А. Воробьев // Теория и практика системного анализа. 2010. Т. I I. Загл. с экрана. Яз. рус.

17 Акулинин, С. А. Выбор параметров LDPC-кодов для каналов с аддитивным белым гауссовским шумом [Электронный ресурс] / С. А. Акулинин, И. В. Свиридова // Вестник Воронежского государственного университета, 2015. Вып. № 6. Загл. с экрана. Яз. рус.

18 William, E. An Introduction to LDPC Codes [Электронный ресурс] / E. William // The University of Arizona, Box 210104, Tucson, AZ 85721, Aug. 2003. Загл. с экрана. Яз. англ.

19 Gallager, R. Low-density parity-check codes [Электронный ресурс] / R. Gallager // IRE Transactions on Information Theory, 8(1), 1962. Загл. с экрана. Яз. англ.

20 Скляр, Б. Цифровая связь. Теоретические основы и практическое применение [Электронный ресурс] / Б. Скляр. М. : Вильямс, 2003, 1104 с. Загл. с экрана. Яз. рус.

21 Та, Т. A tutorial on low density parity-check codes [Электронный ресурс] / Т. Та. Загл. с экрана. Яз. англ.