УДК 621.391.26

ВЕРОЯТНОСТНОЕ ДЕКОДИРОВАНИЕ КОДОВ С ВЫСОКОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА РАСПРОСТРАНЕНИЯ ДОВЕРИЯ

М.А. АЛИСИЕНКО, А.П. ТУРЛАЙ, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 18 февраля 2022

Аннотация. Рассмотрены подходы вероятностного декодирования кодов с высокой плотностью контроля четности на основе алгоритма распространения доверия с жесткими и адаптивными мягкими решениями. Рассмотрены примеры схем декодирования с использованием нейронной сети. Предложена методика оценки сложности декодирования.

Ключевые слова: алгоритм распространения доверия, коды с высокой плотностью проверок на четность, проверочная матрица, нейронная сеть, адаптивный алгоритм декодирования.

Введение

Современные коды, такие как турбокоды, коды LDPC и полярные коды, обычно достигают хорошей производительности только при относительно больших длинах блоков. При коротких и средних длинах блоков коды с высокой плотностью проверок на четность (HDPC), такие как коды BCH и коды Рида-Соломона, могут быть лучшим выбором из-за их свойства высокой корректирующей способности [1–3]. Хотя для таких кодов существуют алгоритмы жесткого решения низкой сложности, эти алгоритмы не достигают полной мощности исправления ошибок, которую имеют короткие коды HDPC при оптимальном декодировании. С другой стороны, по своей природе классические коды имеют очень плотную проверочную матрицу с небольшим обхватом и большим количеством коротких циклов. Поэтому выполнение на них стандартного итеративного декодирования обычно приводит к плохим результатам.

В данной работе рассматриваются алгоритмы построения эффективных итеративных декодеров кодов с высокой плотностью контроля четности.

Вероятностный алгоритм распространения доверия

Алгоритм распространения доверия выполняется на основе векторов, состоящих из вещественных величин, полученных на выходе канала путем пересчета вероятностей через алгоритм распространения доверия (belief propagation decoding). На основе принятого из канала вектора $\mathbf{C}$ формируются два вектора, для двоичного случая, вероятностей того, что в принятом векторе на данной позиции находился заданный символ [3–5].

Каждому ненулевому элементу проверочной матрицы кода присваивают две величины: $q^x_{i,j}$ и $r^x_{i,j}$. Величина $q^x_{i,j}$ является вероятностью того, что j-ый символ принятого вектора имеет значение x по информации, полученной из всех проверок, кроме i-ой. Величина $r^x_{i,j}$ является вероятностью того, что проверка i выполняется, если j-ый символ принятого вектора равен x, а все остальные символы проверок имеют распределение вероятностей, заданное величинами $\left\{q^x_{i,j'} : j' \in N(i) \setminus j\right\}$ где $N(i)$ – множество символов, входящих в i-ю проверку.

Перед началом работы алгоритму требуется инициализация, далее работа идет по принципу пересчета вероятностей символов принятого вектора, используя для пересчета вероятностей правило Байеса для апостериорной вероятности события. Одна итерация алгоритма представляет собой следующую последовательность действий:

1. Для всех проверок вычисляются величины $\Delta r_{i,j}$ и пересчитываются вероятности $r_{i,j}^{x}$ для $x = \{0,1\}$.

2. Для всех символов принятого вектора пересчитываются вероятности $q_{i,j}^{x}$.

3. Формируются векторы псевдоапостериорной вероятности q_j^0 и q_j^1.

4. Формируется вектор решения **C′** по следующему правилу: элемент вектора $c_j = 1$, если q_j^1 больше заданного порогового значения, иначе $c_j = 0$.

5. Если вектор **C′** является кодовым словом, декодирование заканчивается, в противном случае выполняется следующая итерация алгоритма.

Существует несколько алгоритмов мягкого декодирования для кодов HDPC с высокой производительностью одним из которых является адаптивный алгоритм вероятностного декодирования.

Сложность «мягких» алгоритмов выше, чем сложность алгоритма «жесткого» декодирования путем инвертирования битов, но качество декодирования повышается за счет использования дополнительной информации на выходе канала. Однако, точность работы «мягкого» алгоритма зависит от инициализации. Чем точнее инициализация произведена, тем точнее будет конечный результат. Для канала с гауссовским шумом инициализация может быть произведена при помощи информации о дисперсии шума в канале. Для других распределений шума в канале или при неизвестных характеристиках шума точная инициализация алгоритма может оказаться сложной задачей.

Адаптивный алгоритм «мягкого» вероятностного декодирования

Известно несколько алгоритмов мягкого декодирования для кодов HDPC с высокой производительностью, одним из которых является адаптивный алгоритм вероятностного декодирования BP [1, 4].

Модификация алгоритма BP путем использования нейронной сети, значительно улучшает его производительность для кодов HDPC. В нейронном алгоритме BP, сообщения вычисляются так же, как и в традиционном BP на основе LLR, а затем умножаются на набор мультипликативных весов. Веса уникальны для каждой итерации; следовательно, в качестве композиции аффинных преобразований и нелинейностей нейронный декодер BP можно рассматривать как своего рода не полностью связанную нейронную сеть с прямой связью, как показано на рис. 1. Каждый уровень сети состоит из обучаемой операции передачи сообщений.

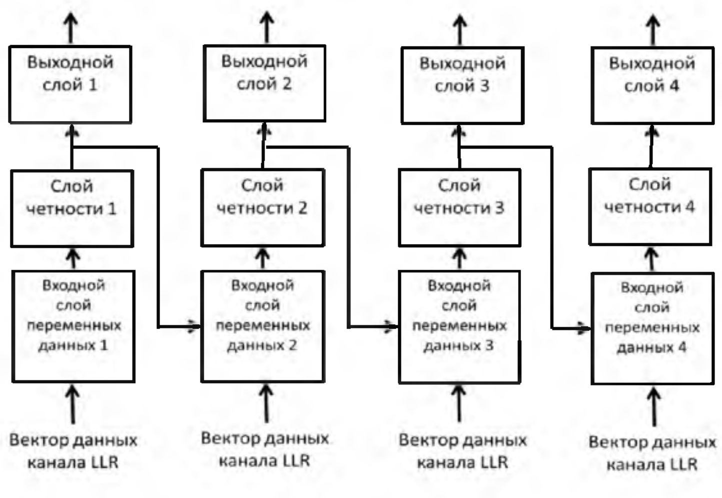

Рис. 1. Декодер на основе не полностью связанной нейронной сети с прямой связью

Нейронный алгоритм BP является примером «глубокого развертывания» [6–8]. Методологически итерационный алгоритм (который может быть или не быть алгоритмом обучения) разворачивается, и каждой итерации назначаются обучаемые параметры, чтобы получить глубокую архитектуру.

Для обучения нейронных декодеров BP может быть использован алгоритм минимизации средней перекрестной энтропии между каждым программным выходом декодера (пропущенным через сигмовидную функцию для получения значений в диапазоне [0, 1]) и каждым соответствующим битом переданного кодового слова.

Возможна модификация алгоритма декодирования «сумма-произведение» (SP). В основе модификации лежит алгоритм адаптации матриц проверки четности от итерации к итерации на основе логарифмического отношения правдоподобия (LLR) входящего сигнала. Аппаратная реализация декодера требует применения алгоритма исключения Гаусса, который используется в каждой итерации SP.

Декодер на основе линейного программирования

Метод интерпретирует проверочную матрицу как набор ограничений и использовали методы линейного программирования для декодирования полученного кодового слова [9].

Декодер линейного программирования (ДЛП) действует на фундаментальном многограннике, созданном ограничениями матрицы проверки четности. Многогранник имеет вершины, которые являются допустимыми кодовыми словами, и вершины, которые являются недопустимыми кодовыми словами. Декодирование линейным программированием в конечном итоге останавливается на одной из вершин, которое называют псевдокодовым словом (ПКС) [10]. Сходство в производительности и аналогичное поведение декодирования ДЛП и распространения доверия (BP) привели к использованию веса и распределения PCW для оценки и улучшения производительности декодирования.

Обогащение структуры матрицы контроля четности путем добавления избыточных строк улучшает функцию распределения веса ПКС и производительность декодирования. Здесь необходимо учитывать, что добавление большего количества строк в матрицу проверки на четность может увеличить количество коротких циклов в графе и снизит производительность его декодирования.

Алгоритмы декодирования используют избыточные матрицы проверки на четность. Один из вариантов декодирования определяет матрицы проверки на четность $(n \times n)$, путем получения их из кодовых слов минимального веса двойственного кода [1]. Возможно использование «временной» избыточной матрицы проверки на четность путем изменения базовой матрица проверки на четность на протяжении всего процесса декодирования. Различная структура избыточных матриц декодеров влияет на вычислительную сложность декодирования [11, 12].

«Временная» избыточность, достигается за счет использования группы изоморфизмов перестановок Per(C), которая определяется как набор перестановок координатных мест, которые переводят код C в себя. Случайным образом выбирая элементы из Per(C), декодер изменяет набор ограничений, которые используются во времени. Этот процесс также можно рассматривать как смену многогранника при очередной попытке приблизиться к решению или как декодирование с переставленным мягким входным вектором, что эквивалентно декодированию с помощью переставленной матрицы контроля четности.

Методика оценки сложности декодирования

Все выражения алгоритма задаются как функции числа ребер двудольного графа, индуцированного кодом. Таким образом, сравнение двух разных декодеров, которые используют разные матрицы проверки на четность, достигается путем нормализации количества ребер их графов.

Если алгоритмы используют одну и ту же матрицу проверки на четность, то сложность декодера оценивается путем усреднения количества итераций суммы-произведения, выполняемых до тех пор, пока не будет достигнуто допустимое кодовое слово или пока количество итераций не достигнет определенного предела в случае, если декодер не сходится к кодовому слову. Одна итерация определяется как действие по отправке сообщений из узлов-переменных в узлы-переменные, обработка этих сообщений в узлах-проверках и отправка новых сообщений из узлов-проверок в узлы-переменные.

Матрица проверки четности **H** для некоторого кода $C(n,k)$ имеет размер $(n \times n)$. Нормируя относительную сложность, можно установить все декодеры в одном масштабе. Количество ребер в графе равно $nd_{\min}$. Относительная сложность – это отношение количества ребер в графах. Сложность алгоритмов можно сравнить, умножив среднее количество итераций суммы-произведения на показатель относительной сложности.

Так, для кода Голея (24, 12, 8) относительную сложность можно оценить, как 1,7. Для кода БЧХ (31, 16, 7) относительная сложность равна 1,5; для кода (63, 45, 7) – относительная сложность равна 3,2. Здесь относительная сложность пропорциональна длине кода.

Заключение

Рассмотрены различные алгоритмы итеративного декодирования кодов с высокой плотностью проверок на четность. Показано, что итерационное адаптивное декодирование позволяет повысить эффективность «мягкого» декодирования таких кодов. Приведена методика и результаты оценки сложности декодирования некоторых кодов.

PROBABILISTIC DECODING OF CODES WITH A HIGH DENSITY OF PARITY CHECKS USING THE BELIEF PROPAGATION ALGORITHM

M.A. ALISIENKO, A.P. TURLAY, S.B. SALOMATIN

Abstract. Approaches for probabilistic decoding of high-density parity codes based on a belief propagation algorithm with hard and adaptive soft decisions are considered. Examples of decoding schemes using a neural network are considered. A technique for estimating the complexity of decoding is proposed algorithm for searching for single-pixel extremes of halftone images based on centrally symmetric scanning is proposed. It is shown that the algorithm works much faster than the best known algorithms for detecting key points of images.

Keywords: belief propagation algorithm, high-density parity-check codes, parity check matrix, neural network, adaptive decoding algorithm.

Список литературы

1. Richardson T., Urbanke R. Modern Coding Theory. Cambridge, UK: Cambridge University Press, 2008.
2. Koetter R., Vardy A. // IEEE Transaction on Information Theory. 2003. Vol. 49. P. 2809–2825.
3. Doan N. [et al.] // arXiv preprint arXiv: 1811. 00124. 2018.
4. Luo F. Machine learning for future wireless communication. Wiley TEEE Press, 2020
5. Tseng H., Wu J. // The International Journal of Electronics.1993. Vol. 75, No. 4. P. 589–594.
6. Liva G. [et al.] // arXiv preprint arXiv: 1610.00873. 2016.
7. O'Shea T., Hoydis J. // IEEE Transactions on Cognitive Communications and Networking. 2017. Vol. 3, No. 4. P. 563–575.
8. Hershey J.R., Le Roux J., Weninger F. // Mitsubishi Electric Research Laboratories. Tech. Rep. 2014. TR2014–117.
9. Feldman J. Decoding Error-Correcting Codes via Linear Programming. PhD dissertation. Massachusetts Institute of Technology. 2003.
10. Kelley C.A., Sridhara D. // IEEE Trans. Inform. Theory. 2007. Vol. 53, No. 11, P. 4013–4038.
11. Fossorier M. P. C., Mihaljevi´c M., Imai H. // IEEE Trans. Commun. 1999. Vol. 47. P. 673–680.
12. Halford T.R. The Extraction and Complexity Limits of Graphical Models for Linear Codes. PhD dissertation. University of Southern California, 2007.
.