

УДК 004.312.26

О.В. Стукач¹, д-р техн. наук, проф.,
А.Н. Романюк², д-р техн. наук, проф.,
А.Я. Кулик², д-р техн. наук, проф.,
Ю.Ю. Иванов², аспирант¹ Томский политехнический университет, г. Томск, Россия² Винницкий национальный технический университет, г. Винница, Украина
ran12345@mail.ru, YuraП@yandex.ru

Снижение вычислительной сложности алгоритма декодирования BCJR MAP в турбо-кодовых конструкциях

Рассматриваются вопросы, связанные с современными методами турбо-кодирования, перспективными для применения в цифровых системах связи. Представлены алгоритмы, которые позволяют снизить вычислительную сложность - \log -MAP, linear-log-MAP и max-log-MAP . Получено обобщенное выражение для вычисления логарифма отношения правдоподобий в процессе этих процедур декодирования. С помощью имитационного моделирования по методу Монте-Карло проведено исследование вероятностно-энергетических характеристик передачи информации в турбо-кодовых конструкциях.

Ключевые слова: турбо-код, декодирование, BCJR алгоритм, аппроксимация, \log -MAP, корректирующая функция, linear-log-MAP , max-log-MAP .

Введение

Теория информации и кодирования зародилась в работах [1] американского инженера К. Шеннона в 1948 г. Он предложил использовать компрессию данных с источника, шифровать данные, а затем применять помехоустойчивое кодирование (ПК), дальнейшее развитие которого связано с работами А. Колмогорова, В. Котельникова, Р. Хеминга, П. Элайеса, Р. Галлагера, И. Рида, Г. Соломона, Д. Форни, К. Берру, Д. Маккея и других ученых, которые решили различные проблемы в области передачи информации, разработав технологии, которые позволяют достичь рекордных показателей BER (Bit Error Rate - вероятность ошибки на бит). Совершенствование средств защиты информации на основе ПК особенно важно и актуально.

Революционным событием в ПК стала фундаментальная работа 1993 года [2], в которой французские ученые под руководством К. Берру представили термин "турбо" и математический аппарат для работы с параллельной каскадной конкатенацией сверточных кодов (ПККСК или турбо-код). Созданная конструкция, которая представляет собой способ построения случайного кода большой длины, позволила приблизиться к идеальному по К. Шеннону коду. Её главный принцип - использование двух (двумерный код) или более (многомерный код) параллельно работающих компонентных кодеров. При этом информационный блок кодируется несколько раз по количеству примененных в

системе кодов, причем второй и последующие кодеры осуществляют процедуру кодирования только после предварительного перемешивания битов (interleaving) по определенному алгоритму. Необходимо заметить, что алгоритмы декодирования применяются с использованием демодулятора с мягкими решениями, что позволяет достичь максимально возможного энергетического выигрыша от декодирования [3].

Турбо-коды позволяют увеличить скорость передачи информации, не требуя увеличения мощности передатчика, а также они могут быть использованы для уменьшения необходимой мощности при передаче с заданной скоростью, что, безусловно, делает их применение перспективным [3, 4].

Турбо-подобные конструкции с вероятностными алгоритмами декодирования позволяют осуществить высокоэффективную передачу данных практически в любой системе связи - телевидении, мобильных и космических коммуникациях, к примеру, исследования NASA JPL (Mars Reconnaissance Orbiter + Mars Science Laboratory) позволили получить 24 Гб информации, включая высококачественные фотографии поверхности Красной планеты с помощью марсохода Curiosity. Для передачи данных использовалась схема ПККСК ($R = 1/6$, $k = 8920$ бит). В биоинформатике и генетике для работы с ДНК также используются подобные конструкции наряду с кодом Рида-Соломона. Если необходимо работать с объемными сообщениями на высоких скоростях

передачи данных, то применяют турбо-коды, LDPC, RA-коды, которые при переходе к итеративным процедурам декодирования информации по своим характеристикам максимально приближаются к границе К. Шеннона.

Прием и формирования турбо-кода с использованием вычислительной мощности технических устройств, реализация разработанных вычислительных процедур для работы с данным кодом в технике, а также исследования вероятностно-энергетических характеристик процесса передачи информации с использованием технических средств при работе с турбо-кодами являются актуальными проблемами.

Постановка задачи

Создание ПК тесно связано с алгоритмами декодирования. Почти все коды могут декодироваться только переборными методами, при этом вариантов решения больше числа атомов во Вселенной. Поэтому необходимо **найти и исследовать** методы непереборного декодирования, **обеспечить** качество декодирования, учитывая условия реальных систем связи.

Одним из наиболее мощных алгоритмов вероятностного декодирования является алгоритм BCJR. Идея работы декодера турбо-кодовой системы заключается в модификации алгоритма, который впервые представили в 1974 году L. Bahl, J. Cocke, F. Jelinek и J. Raviv [5]. В англоязычных источниках такой алгоритм имеет несколько названий: BCJR (по первым буквам фамилий авторов), MAP (по максимуму апостериорной вероятности), APP (по апостериорной вероятности), Forward-Backward (алгоритм вперед-назад), Belief Propagation (алгоритм с распространением доверия), Sum-Product (алгоритм суммы произведений). В работе [6] П. Робертсон и соавторы создали оптимальный *log*-MAP и субоптимальный *max-log*-MAP алгоритмы декодирования. Данные модификации упрощают вычислительную сложность BCJR MAP алгоритма. В процессе работы *log*-MAP алгоритма необходимо вычислять корректирующую функцию $f_{кор}$, поэтому актуальной задачей является аппроксимация $f_{кор}$ с целью упростить вычисления.

Сложность алгоритмов турбо-кодирования и явная недостаточность программного обеспечения свободного распространения препятствуют внедрению турбо-кодов, хотя в настоящее время многие системы используют именно их. При работе с рассмотренным кодом

возникает проблема его декодирования, а, соответственно, и реализации этой процедуры. Таким образом, необходимо определить особенности алгоритмов, снижающих сложность декодирования турбо-кодов. Существует определенное количество научных работ, которые оказывают идеи для решения представленных проблем, например, [6 - 9] или другие, связанные с данной тематикой.

Решение поставленной задачи

Рассмотрим алгоритм BCJR для общего случая марковского источника информации, которая передается через дискретный канал без памяти [7, 8]. Этот метод является оптимальным алгоритмом посимвольного MAP-декодирования линейных блочных кодов, который минимизирует BER. Идея MAP-декодирования состоит в вычислении апостериорных вероятностей информационных символов, используя заданную принятую последовательность \bar{r} и LLR (log-likelihood ratio - логарифм отношения правдоподобия), что можно записать в формуле

$$LLR(\bar{U}_i) = \log \left(\frac{p(\bar{U}_i = 1 | \bar{r})}{p(\bar{U}_i = 0 | \bar{r})} \right), \quad (1)$$

где \bar{U}_i – информационный символ.

Обобщенное выражение для вычисления LLR процедуры MAP-декодирования в алгоритме BCJR имеет вид

$$LLR(\bar{U}_i) = \log \left(\frac{\sum_m \sum_{m'} \alpha_{i-1}(m') \cdot \gamma_i^{(1)}(m', m) \cdot \beta_i(m)}{\sum_m \sum_{m'} \alpha_{i-1}(m') \cdot \gamma_i^{(0)}(m', m) \cdot \beta_i(m)} \right), \quad (2)$$

где $\alpha_i(m) = \sum_{m'} \alpha_{i-1}(m') \cdot \sum_{j=0}^1 \gamma_i^{(j)}(m', m)$ – метрика

прямого пути на треллис (решетке сверточного кода); $\gamma_i^{(j)}(m', m)$ – метрика ребра (транзитная);

$\beta_i(m) = \sum_{m'} \beta_{i+1}(m') \cdot \sum_{j=0}^1 \gamma_i^{(j)}(m', m)$ – метрика

обратного пути на треллис.

Для того, чтобы снизить вычислительную сложность MAP алгоритма, могут быть использованы логарифмы метрик. Алгоритм, который использует такой переход, называют *log*-MAP алгоритмом [7, 8]. В дальнейших формулах применяется натуральный логарифм, но

используется обозначение \log по названию метода декодирования. На основе уравнения для вычисления метрики прямого пути на решетке кода, можно получить выражение

$$\log a_i(m) = \log \left(\sum_{m'} \sum_{j=0}^1 \exp(\log a_{i-1}(m') + \log \gamma_i^j(m', m)) \right). \quad (3)$$

Аналогично, используя формулу для получения метрики обратного пути на треллис-диаграмме кода, можно найти выражение

$$\log \beta_i(m) = \log \left(\sum_{m'} \sum_{j=0}^1 \exp(\log \beta_{i+1}(m') + \log \gamma_i^{(j)}(m', m)) \right). \quad (4)$$

Вероятность $\gamma_i^{(j)}(m', m)$, которая называется метрикой ребра или транзитной метрикой, в дискретном гауссовском канале будет иметь вид

$$\gamma_i^{(j)}(m', m) = p\{\overline{U}_i = j\} \cdot \delta_{ij}(m, m') \times \exp \left(-\frac{1}{N_0} \cdot \sum_{q=0}^{N-1} (\overline{r}_{i,q} - \overline{X}_{i,q})^2 \right), \quad (5)$$

где $\overline{U}_i = j$ – информационный бит с множества $\Theta_i^{(j)}$ ребер, которые связывают состояния $S_i^{(m)}$ и $S_{i-1}^{(m')}$, $j \in \{0, 1\}$; $\overline{X}_{i,q}$ – переданный символ; $\overline{r}_{i,q}$ – принятое значение; $\delta_{ij}(m, m') = 1$, если $\{m, m'\} \in \Theta_i^{(j)}$; $\delta_{ij}(m, m') = 0$, если $\{m, m'\} \notin \Theta_i^{(j)}$; $\frac{E_b}{N_0}$ – отношение сигнал / шум на бит.

Если взять логарифм величины $\gamma_i^{(j)}(m', m)$ в формуле (5) и произвести сокращения выражения, то получим

$$\log \gamma_i^{(j)}(m', m) = \delta_{ij}(m, m') \times \left\{ \log p\{\overline{U}_i = j\} - \frac{1}{N_0} \cdot \sum_{q=0}^{N-1} (\overline{r}_{i,q} - \overline{X}_{i,q})^2 \right\}. \quad (6)$$

Тогда, если ввести обозначения $Y_i^{(j)}(m', m) = \log \gamma_i^{(j)}(m', m)$, $A_i(m) = \log a_i(m)$, $B_i(m) = \log \beta_i(m)$, то выражение (2) запишем в

сокращенном виде для процедуры \log -MAP декодирования

$$LLR(\overline{U}_i) = \log \left[\frac{\sum_{m'} \sum_{m''} \exp(A_{i-1}(m') + Y_i^{(1)}(m', m) + B_i(m))}{\sum_{m'} \sum_{m''} \exp(A_{i-1}(m') + Y_i^{(0)}(m', m) + B_i(m))} \right]. \quad (7)$$

В результате преобразований и упрощений получили алгоритм MAP, используемый в логарифмической форме. Для того, чтобы избежать операции суммы для экспоненциальных составляющих, можно применить логарифм якобиана [7], формула для определения которого имеет вид

$$\begin{aligned} \log(\exp(\Omega) + \exp(\Psi)) &= \\ &= \max(\Omega, \Psi) + \log(1 + \exp(-|\Omega - \Psi|)) = \\ &= \max(\Omega, \Psi) + f(|\Omega - \Psi|), \end{aligned} \quad (8)$$

где $f_{\text{кор}} = f(|\Omega - \Psi|) = \log(1 + \exp(-|\Omega - \Psi|))$.

Для упрощения, экономии времени и скорости вычислений, вместо того, чтобы несколько раз обращаться к относительно медленной и дорогой в аппаратном выполнении функции $\exp(x)$ для выражения $f(|\Omega - \Psi|)$ составляют таблицу 1 [9]. Известно, что всего несколько значений достаточно, чтобы почти достичь точности MAP алгоритма.

Таблица 1 – Значения функции $f(|\Omega - \Psi|)$

$ \Omega - \Psi $	$f(\Omega - \Psi)$
0,000	0,693
0,125	0,633
0,250	0,576
0,500	0,474
1,000	0,313
2,000	0,127
4,000	0,018
8,000	0,0003
∞	0,000

Возможно также выполнить аппроксимацию корректирующей функции. Вид графика функции $f(|\Omega - \Psi|)$ показан на рис. 1, где f_j (\log -MAP) – рассматриваемая функция, approx_j (linear-log-MAP) – функция, полученная с помощью аппроксимации линейной функцией по методу наименьших квадратов, j – количество измерений для моделирования при шаге h ,

который для аргумента $|\Omega - \Psi|$ имеет значение 0,2. Таким образом, получены коэффициенты для линейной функции $\alpha = -0,205$ и $b = 0,572$, то есть $f_{кор} = b + \alpha \cdot j$.

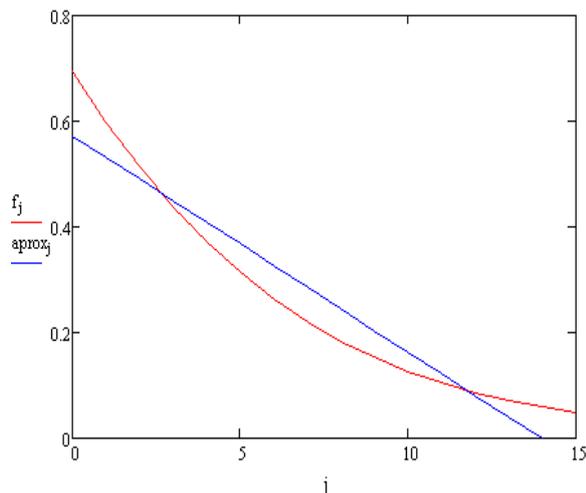


Рисунок 1 – Корректирующие функции для log -MAP и $linear$ - log -MAP алгоритмов

Для уменьшения вычислительной сложности, но с потерей свойства оптимальности используется модифицированный MAP алгоритм, известный как max - log -MAP. Сущность этой модификации состоит в том, что логарифмируется MAP метрика и применяется аппроксимация вида

$$\log(\exp(\Omega) + \exp(\Psi)) \approx \max(\Omega, \Psi). \quad (9)$$

В результате, используя формулу (9) и свойства логарифма дроби, полученное выражение логарифма отношения правдоподобия для информационного символа \overline{U}_i приобретает вид

$$\begin{aligned} LLR(\overline{U}_i) \approx & \max_{m',m} \{A_{i-1}(m') + Y_i^{(1)}(m',m) + B_i(m)\} - \\ & - \max_{m',m} \{A_{i-1}(m') + Y_i^{(0)}(m',m) + B_i(m)\}. \end{aligned} \quad (10)$$

Вычисления на прямом и обратном путях могут быть представлены в следующем виде

$$A_i(m) = \max_{m'} \max_{j \in \{0,1\}} \{A_{i-1}(m') + Y_i^{(j)}(m',m)\}, \quad (11)$$

$$B_i(m) = \max_{m'} \max_{j \in \{0,1\}} \{B_{i+1}(m') + Y_i^{(j)}(m',m)\}. \quad (12)$$

Для моделирования алгоритмов $linear$ - log -MAP и max - log -MAP (рис. 2 и 3) методом Монте-Карло в среде MatLab использован турбо-код с кодовой скоростью $R = \frac{1}{3}$ (rate), два рекурсивных систематических сверточных кодера на порождающих полиномах $\{7,5\}_8$, длина блока $k = 480$ бит (frame size), BPSK модуляция, канал с AWGN, перемежитель типа random, критерий остановки процесса декодирования на основе максимального числа итераций (8 итераций). Результаты показаны на графиках зависимости вероятности ошибки на бит BER от отношения сигнал / шум на бит $\frac{E_b}{N_0}$.

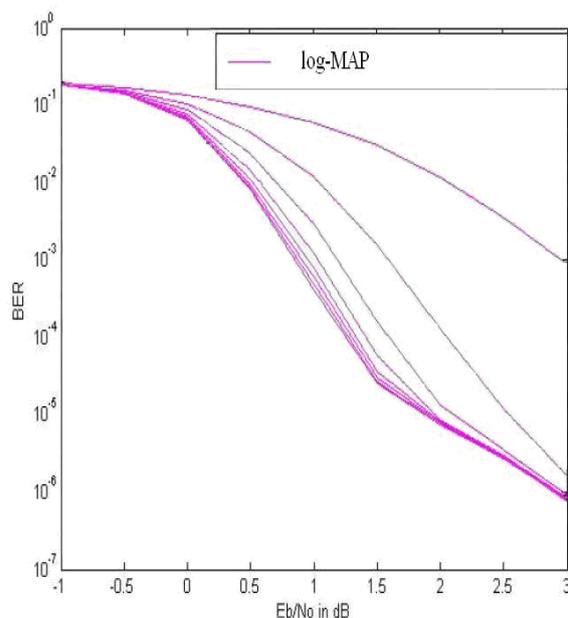


Рисунок 2 – Моделирование BER для алгоритма $linear$ - log -MAP методом Монте-Карло

Сложность алгоритма log -MAP примерно вдвое больше, чем для max - log -MAP. Для алгоритмов log -MAP и MAP вероятность ошибки минимальна и одинакова.

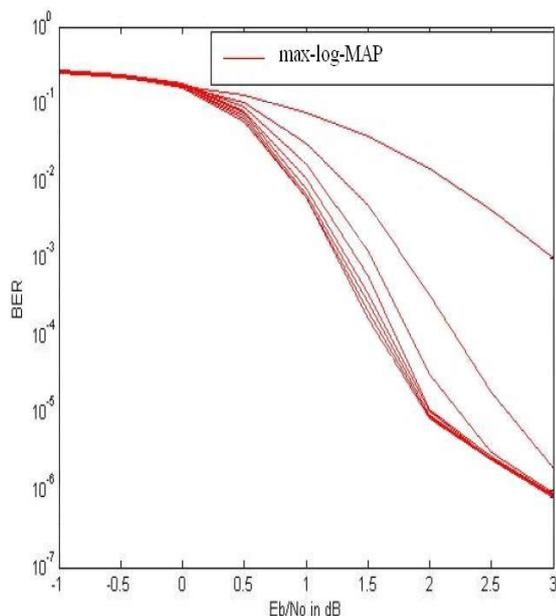


Рисунок 3 — Моделирование BER для алгоритма *max-log-MAP* методом Монте-Карло

Заклучение

Таким образом, для эффективного использования информации, полученной с каждого декодера, применяют "мягкую" схему декодирования, поскольку в каскадной схеме, такой как турбо-код, для надежной работы алгоритм декодирования не должен быть ограничен представлением на декодеры "жесткой" схемы решений. Оптимальными являются алгоритм MAP-декодирования турбо-кодов и его модификация *log-MAP*. Можно рассматривать также алгоритмы с аппроксимацией корректирующей функции, например *linear-log-MAP*. Алгоритм декодирования *max-log-MAP* не требует использования функции-корректора, но является субоптимальным. Эти методы значительно снижают вычислительную сложность процесса декодирования, используя логарифм якобиана и его аппроксимации. Представленные алгоритмы могут быть использованы для построения аппаратно-программных средств декодирования сигналов в системах связи. Проведенные исследования подтверждают перспективность использования турбо-кодов в программируемых распределенных компьютерных системах различного функционального назначения.

Список использованной литературы

1. Shannon C.E. A Mathematical Theory of Communication / C.E. Shannon // Reprinted from The Bell System Technical Journal. – 1948. – V. 27. – P. 379–423, 623–656.
2. Berrou C. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes / C. Berrou, A. Glavieux, P. Thitimajshima // IEEE Transactions on Information Theory. – 1996. – V. 44. – № 10. – P. 1064-1070.
3. Иванов Ю.Ю. О некоторых аспектах итеративной стратегии декодирования турбо-кодов: ретроспектива и "турбо"-принцип / Ю.Ю. Иванов, А.Я. Кулик // «Информационные технологии и компьютерная инженерия (ИТКИ)»: матер. IV международной научно-практической конференции. – Винница: ВНТУ, 28-30 мая, 2014 года. – 2014. – С. 157-160.
4. Hanzo L. Turbo Coding, Turbo Equalisation and Space-Time Coding for Transmission over Wireless Channels / L. Hanzo, T.H. Liew, B.L. Yea. – Southampton: Department of Electronics and Computer Science of UK, 2002. – 746 p.
5. Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate / L. Bahl, J. Cocke, F. Jelinek, J. Raviv // IEEE Transactions on Information Theory. – 1974. – V. 20. – P. 284-287.
6. Robertson P. Optimal and Sub-Optimal Maximum A Posteriori Algorithms Suitable for Turbo Decoding / P. Robertson, P. Villebrun, P. Hoeher // European Transactions on Telecommunications. – 1997. – V. 8. – P. 119-125.
7. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. – М.: Техносфера, 2005. – 320 с.
8. Soleymani M.R. Turbo Coding for Satellite and Wireless Communications / M.R. Soleymani, Y. Gao, U. Vilaipornsawai. – New York: Kluwer Academic, 2002. – 231 p.
9. Valenti M. An Efficient Software Radio Implementation of the UMTS Turbo Codec [Web resource] / M. Valenti. – Access mode: <http://www.csee.wvu.edu/~mvalenti/documents/valenti2001c.pdf>.

Надійшла до редакції 18.03.2015

О.В. СТУКАЧ¹, А.Н. РОМАНИУК², А.Я. КУЛИК², Ю.Ю. ІВАНОВ²¹ Томський політехнічний університет, м. Томськ, Росія² Вінницький національний технічний університет, м. Вінниця, Україна**ЗНИЖЕННЯ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ АЛГОРИТМУ ДЕКОДУВАННЯ ВСJR MAP В ТУРБО-КODOVИХ КОНСТРУКЦІЯХ**

Розглядаються питання, пов'язані з сучасними методами турбо-кодування, перспективними для застосування в цифрових системах зв'язку. Представлені алгоритми, які дозволяють знизити обчислювальну складність - *log-MAP*, *linear-log-MAP* і *max-log-MAP*. Отримано узагальнений вираз для обчислення логарифма відношення правдоподібностей в процесі цих процедур декодування. За допомогою імітаційного моделювання по методу Монте-Карло проведено дослідження ймовірнісно-енергетичних характеристик процесу передавання інформації в турбо-кодових конструкціях.

Ключові слова: *турбо-код, декодування, ВСJR алгоритм, апроксимація, log-MAP, коригуюча функція, linear-log-MAP, max-log-MAP.*

O.V. STUKACH¹, A.N. ROMANYUK², A.Ya. KULYK², Yu.Yu. IVANOV²¹ Tomsk Polytechnic University, Tomsk, Russia² Vinnitsa National Technical University, Vinnitsa, Ukraine**REDUCTION COMPUTATIONAL COMPLEXITY OF THE BCJR MAP DECODING ALGORITHM FOR TURBO CODING CONSTRUCTIONS**

The problems associated with modern methods of turbo coding promising for application in digital communication systems are considered. The algorithms, which can reduce computational complexity - *log-MAP*, *linear-log-MAP* and the *max-log-MAP*, are presented. Generalized expression for calculating the logarithm of likelihood ratio during decoding procedures is obtained. Using modeling by Monte-Carlo method the research of probabilistic and energy characteristics for information transfer process in turbo coding constructions is performed.

Keywords: *turbo code decoding, BCJR algorithm, approximation, log-MAP, correcting function, linear-log-MAP, max-log-MAP.*