Реализация алгоритма декодирования методом рандомизированного правдоподобия с мягкими решениями

А. Д. Лебединская

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

E-mail: lad6575@mail.ru

К. Б. Шабунов

Московская лаборатория алгоритмов радиосвязи

E-mail: k.shabunov@rtt-lab.ru

Аннотация. **Предлагается метод декодирования для произвольного линейного кода в полунепрерывном канале связи. Метод основан на реализации принципа рандомизированного правдоподобия (Randomized Likelihood – RL) путем выборки с отклонением (Rejection Sampling – RS). В отличие от существующих реализаций, используется выход канала связи с мягкими решениями. Представлены результаты сравнения предложенного алгоритма с оптимальным декодером.**

Ключевые слова: декодирование, линейный код, выборка с отклонением, рандомизированный алгоритм

I. Введение

На сегодняшний день, из-за движения технологий связи в сторону уменьшения задержки при передаче данных, новые методы декодирования для кодов малой и средней длины становятся все более востребованными. Особый интерес направлен на общие методы декодирования, которые могут работать с произвольным линейным кодом. Исходя из этого, в данной статье предлагается реализация декодера по принципу рандомизированного правдоподобия (Randomized Likelihood – RL), которая сравнима с оптимальным декодером, основанным на принципе максимального правдоподобия (Maximum Likelihood – ML).

A. Оптимальный декодер

Рассмотрим стандартную модель передачи информации через канал связи. На вход подается двоичная информационная последовательность, которая разбивается на информационные блоки $\mathbf{m} = (m_1, m_2, ..., m_k)$ длины k, где m_i принимают значения либо 0, либо 1. При кодировании двоичным кодом каждому такому блоку сопоставляется кодовое слово вида $\mathbf{x}(\mathbf{m}) = (x_1, x_2, ..., x_n)$, где x_i также принимают значения 0 или 1. Мы будем рассматривать линейные коды, поэтому $\mathbf{m}$ и образованное от него $\mathbf{x}$ связаны через порождающую матрицу $\mathbf{G}$ размером $k \times n$ выражением

$$\mathbf{x}(\mathbf{m}) = \mathbf{m}\mathbf{G}.$$

Оптимальное декодирование, минимизирующее вероятность ошибки на блок (block error rate – BLER), реализуется правилом максимума апостериорной вероятности (Maximum a posteriori probability – MAP):

$$\hat{\mathbf{m}}_{\text{MAP}}(\mathbf{y}) = \arg\max_{\mathbf{m}} p(\mathbf{m} \mid \mathbf{y}), \qquad (1)$$

где $\hat{\mathbf{m}}$ – результат работы декодера, $p(\mathbf{m} \mid \mathbf{y})$ – апостериорная вероятность события, в котором при выходе канала $\mathbf{y}$ информационным блоком являлось $\mathbf{m}$.

При равновероятном распределении символов в информационной последовательности выражение (1) эквивалентно правилу максимального правдоподобия (Maximum Likelihood – ML):

$$\hat{\mathbf{m}}_{\text{ML}}(\mathbf{y}) = \arg\max_{\mathbf{m}} p\left(\mathbf{y} \mid \mathbf{x}(\mathbf{m})\right),$$

где $p\left(\mathbf{y} \mid \mathbf{x}(\mathbf{m})\right)$ – условная вероятность получения выхода канала $\mathbf{y}$ при условии того, что передавалось сообщение $\mathbf{m}$.

В аддитивном канале данное правило сводится к декодированию по минимальному расстоянию, когда находится $\hat{\mathbf{m}}$, минимизирующее расстояние Хэмминга $d_H\left(\mathbf{x}(\mathbf{m}), \bar{\mathbf{y}}\right)$ в канале с жесткими решениями (для каждого переданного сигнала детектор принимает решение о том, передавался ли сигнал, соответствующий 0 или 1, и передает двоичный вектор $\bar{\boldsymbol{y}}$ на вход декодера), или евклидово расстояние $d\left(\mathbf{z}(\mathbf{m}), \mathbf{y}\right)$ в канале с мягкими решениями. Тривиальная реализация такого подхода требует полного перебора 2^k возможных комбинаций.

Поиск наиболее эффективной реализации оптимального декодирования продолжается до сих пор. Уже довольно давно известно, что задача декодирования произвольного кода по максимуму правдоподобия имеет экспоненциальную сложность от n [1], поэтому сейчас фокус большинства исследований сместился в сторону разработки способов уменьшения сложности декодирования без серьезного увеличения вероятности неправильного декодирования.

B. Рандомизированное декодирование

Ввиду описанного в предыдущем пункте, в работе [1] было предложено рассмотреть подоптимальное правило рандомизированного правдоподобия (Randomized Likelihood – RL), при котором оценка информационного сообщения получается как случайный вектор, выбранный из реализации апостериорного распределения

$$\hat{\mathbf{M}}_{\text{RL}} \sim p(\mathbf{m} \mid \mathbf{y}). \qquad (1)$$

В работе [3] доказано, что вероятность неправильного декодирования по принципу RL превышает вероятность ошибки оптимального декодирования не более чем в 2 раза, т. е.

$$p\left(\mathbf{M} \neq \hat{\mathbf{M}}_{\mathrm{RL}}(\mathbf{Y})\right) \leq 2\,p\left(\mathbf{M} \neq \hat{\mathbf{m}}_{\mathrm{ML}}(\mathbf{Y})\right). \qquad (2)$$

Эта граница гарантирует высокую корректирующую способность RL декодера, проблема же заключается в реализации выборки из апостериорного распределения (1). В работе [2] было предложено несколько вариантов решения этой задачи путем адаптации известных общих методов сэмплирования. Дальнейшее развитие этот подход получил в [4].

II. Декодирование на основе выборки с отклонением

Алгоритм выборки с отклонением (Rejection Sampling – RS) основан на получении сложного целевого распределения $p(v)$ с помощью более простого вспомогательного $q(v)$. Для этих распределений выбираются нормирующие коэффициенты Z_p и Z_q, такие что для $p^*(v) = p(v) \cdot Z_p$ и $q^*(v) = q(v) \cdot Z_q$ всегда выполняется условие

$$\frac{p^*(v)}{q^*(v)} \leq 1.$$

Алгоритм выборки с отклонением генерирует две независимые случайные величины: v из распределения $q(v)$ и u, равномерно распределенное от 0 до 1. Если $u \leq \frac{p^*(v)}{q^*(v)}$, то v принимается как результат работы алгоритма, в противном случае v отклоняется, и генерируются новые v и u. Заметим, соответственно, что время работы этого алгоритма является случайной величиной.

В нашем случае v будет представлять собой информационный вектор $\mathbf{m}$, а $p^*(v)$ будет представлена апостериорной вероятностью от принятого сообщения, т. е. $p(\mathbf{y} \mid \mathbf{m}) = p\left(\mathbf{y} \mid \mathbf{x}(\mathbf{m})\right)$.

A. Выборка с отклонением для ДСК

В работе [2] рассматривается реализация описанного выше алгоритма для двоичного симметричного канала (ДСК). В этом случае искомая апостериорная вероятность записывается как

$$p\left(\mathbf{y} \mid \mathbf{x}(\mathbf{m})\right) = \left(\frac{p}{1-p}\right)^{d_H\left(\mathbf{x}(\mathbf{m}),\bar{\mathbf{y}}\right)} (1-p)^n, \qquad (3)$$

где p – переходная вероятность.

В качестве вспомогательного распределения было предложено использовать апостериорное распределение

$$q\left(\mathbf{m} \mid \bar{\mathbf{y}}_{\mathrm{sys}}\right) = \left(\frac{p}{1-p}\right)^{d_H\left(\mathbf{m},\bar{\mathbf{y}}_{\mathrm{sys}}\right)} (1-p)^k, \qquad (4)$$

где $\bar{\mathbf{y}}_{\mathrm{sys}}$ – вектор жестких решений на выходе канала связи, расположенных на позициях информационных символов кодового слова.

Также было выведено среднее число итераций, требуемых для срабатывания выборки с отклонением:

$$N = 2^{-k} \sum_{\mathbf{y}} Z_q(\mathbf{y}). \qquad (5)$$

Для уменьшения количества итераций было предложено принять нормирующий коэффициент равным $Z_q = (1-p)^{n-k}$, при котором выражение (5) принимает вид

$$N = \left(2 \cdot (1-p)\right)^{n-k}. \qquad (6)$$

В таком случае принятие случайного сообщения $\mathbf{m}$ в качестве результата будет выполняться по следующему условию для проверочных символов:

$$u \leq \left(\frac{p}{1-p}\right)^{d_H\left(\mathbf{x}_{\mathrm{parity}}(\mathbf{m}),\bar{\mathbf{y}}_{\mathrm{parity}}\right)}. \qquad (7)$$

Так как данный алгоритм работает с жесткими решениями, то вероятность неправильного декодирования не превышает двукратной вероятности ошибки оптимального декодера по жестким решениям (Maximum Likelihood HD).

B. Выборка с отклонением с мягкими решениями

В полунепрерывном канале декодирование с жесткими решениями существенно проигрывает декодированию с мягкими решениями. В данной работе предлагается модификация алгоритма из [2], описанного выше, для учета мягких решений (SD). В новом методе предлагается использовать логарифмические отношения правдоподобия (ЛОП), вычисленные исходя из полученного выхода канала. Идея их применения заключается в том, что вместо использования вероятности неправильного принятия жесткого решения для канала в среднем будет произведена оценка этой вероятности для каждой позиции кодового слова индивидуально.

Выражения для ЛОП и разности функций правдоподобия [5] выглядят следующим образом:

$$\mathcal{L}_i = \log \frac{p\left(z_i = +1 \mid y_i\right)}{p\left(z_i = -1 \mid y_i\right)}, \qquad (8)$$

$$S_i = p\left(z_i = +1 \mid y_i\right) - p\left(z_i = -1 \mid y_i\right) = \tanh\left(\frac{\mathcal{L}_i}{2}\right). \qquad (9)$$

Для получения нового выражения для вероятности неправильного приема бита нужно рассмотреть две ситуации: $y_i \geq 0$ и $y_i < 0$ с использованием формул (8) и (9). В первом варианте это вероятность $p(z_i = -1 \mid y_i)$, а во втором – $p(z_i = +1 \mid y_i)$.

При $y_i \geq 0$ значение $p(z_i = -1 \mid y_i)$ можно выразить как

$$p(z_i = -1 \mid y_i) = \tfrac{1}{2}\big[p(z_i = -1 \mid y_i) + p(z_i = +1 \mid y_i) + \\ + p(z_i = -1 \mid y_i) - p(z_i = +1 \mid y_i)\big] = \tfrac{1}{2}\left(1 - \tanh\left(\frac{\mathcal{L}_i}{2}\right)\right).$$

Получается, что

$$p(z_i = -1 \mid y_i) = \tfrac{1}{2}\left(1 - \tanh\left(\frac{\mathcal{L}_i}{2}\right)\right). \qquad (10)$$

При условии, что $y_i < 0$, значение $p(z_i = +1 \mid y_i)$ можно выразить как

$$p(z_i = +1 \mid y_i) = \tfrac{1}{2}\big[p(z_i = -1 \mid y_i) + p(z_i = +1 \mid y_i) + \\ + p(z_i = +1 \mid y_i) - p(z_i = -1 \mid y_i)\big] = \tfrac{1}{2}\left(1 + \tanh\left(\frac{\mathcal{L}_i}{2}\right)\right).$$

Приведенное выше выражение выше сокращается до

$$p(z_i = +1 \mid y_i) = \tfrac{1}{2}\left(1 - \tanh\left(-\frac{\mathcal{L}_i}{2}\right)\right). \qquad (11)$$

Тогда, исходя из (10) и (11), общая формула для вероятности неправильного приема бита записывается как

$$p = \tfrac{1}{2}\left(1 - \tanh\left(\frac{|\mathcal{L}_i|}{2}\right)\right). \qquad (12)$$

Теперь выражения (3) и (4) переписываются в виде

$$p\big(\mathbf{y} \mid \mathbf{x}(\mathbf{m})\big) = \prod_{\substack{i \in [1,\, n] \\ i:\, x_i \neq y_i}} p_i \cdot \prod_{\substack{i \in [1,\, n] \\ i:\, x_i = y_i}} (1 - p_i),$$

$$q\big(\mathbf{m} \mid \bar{\mathbf{y}}_{\text{sys}}\big) = \prod_{\substack{i \in [1,\, k] \\ i:\, m_i \neq y_i}} p_i \cdot \prod_{\substack{i \in [1,\, k] \\ i:\, m_i = y_i}} (1 - p_i). \qquad (13)$$

Если новый нормирующий коэффициент принять равным $Z_q = \prod_{i \in [k+1,\, n]} (1 - p_i)$, условие (7) для срабатывания выборки с отклонением преобразуется в

$$u \leq \prod_{\substack{i \in [k+1,\, n] \\ i:\, x_i \neq y_i}} \frac{p_i}{1 - p_i}. \qquad (14)$$

III. Результаты моделирования

В данном разделе представлены результаты моделирования алгоритмов, описанных в предыдущем разделе.

Моделирование выполнялось в двоичном гауссовом канале с использованием биполярной модуляции. В этом случае передаче кодового слова по каналу соответствует преобразование

$$\mathbf{y} = \mathbf{z} + \mathbf{n},$$

где $\mathbf{n}$ – вектор шума, а элементы вектора $\mathbf{z}$ выражаются как

$$z_i = \begin{cases} +1, & x_i = 0, \\ -1, & x_i = 1. \end{cases}$$

Для моделирования алгоритма из работы [2] переходная вероятность вычислялась как вероятность битовой ошибки эквивалентного ДСК в соответствии с [6]:

$$p = Q\left(\sqrt{2R \cdot SNR}\right),$$

где $Q(x) = \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du$, $R = \frac{k}{n}$ – скорость кода, а *SNR* – отношение сигнал/шум, выраженное в разах [6].

Для алгоритма с мягкими решениями в гауссовском канале ЛОП вычислялись следующим образом:

$$\mathcal{L}_i = \frac{2y_i}{\sigma^2}.$$

где $\sigma = \frac{1}{\sqrt{2R \cdot SNR}}$ – среднее квадратичное отклонение шума.

На рис. 1 и рис. 2 приведены графики, представляющие зависимость вероятности блоковой ошибки (BLER) от отношения сигнал/шум в децибелах (E_b/N_0, dB) для расширенного кода Голея и кода Рида–Маллера RM (2, 5), с параметрами (24, 12) и (32, 16), соответственно. Кривые приведены для двух алгоритмов: метод рандомизированного правдоподобия на основе выборки с отклонением (RL-RS) и метод максимального правдоподобия (ML). Оба варианта также рассмотрены в канале с жесткими (HD) и мягкими решениями (SD).

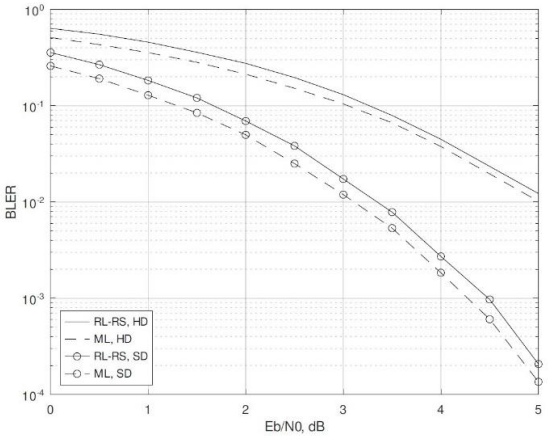

Рис. 1. Вероятность блоковой ошибки для кода Голея (24, 12)

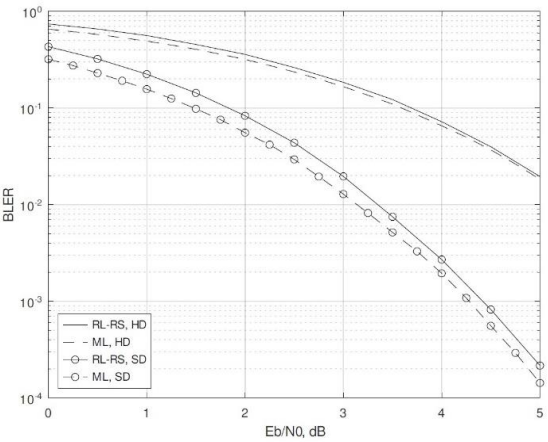

Рис. 2. Вероятность блоковой ошибки для кода RM (32, 16)

Можно наблюдать, что для обоих рассмотренных кодов действительно выполняется правило (2), и введенное использование мягких решений в виде учета ЛОП приближает вероятность ошибки декодирования по методу рандомизированного правдоподобия к оптимальным результатам с небольшим проигрышем (примерно 0,2 дБ в обоих случаях).

IV. Заключение

В данной статье были рассмотрены некоторые реализации декодирования произвольного линейного кода на основе метода рандомизированного правдоподобия, который можно рассматривать как альтернативу использования декодирования по максимуму правдоподобия. Один из алгоритмов для канала с жесткими решениями из работы [2] был обобщен для работы в канале с мягкими решениями. Экспериментальные результаты в АБГШ-канале, полученные для кода Голея (24, 12) и Рида–Маллера (32, 16), показывают малый проигрыш предложенной реализации по BLER по сравнению с оптимальным алгоритмом. В итоге можно сделать вывод, что дальнейший анализ и развитие такого метода декодирования представляет большой интерес для исследований.

Список литературы

[1] E. Berlekamp, R. McEliece and H. van Tilborg, "On the inherent intractability of certain coding problems (Corresp.)," // in IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386, May 1978.

[2] A. Bhatt, J.-T. Huang, Y.-H. Kim, J.J. Ryu and P. Sen, "Monte Carlo Methods for Randomized Likelihood Decoding," // 2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2018, pp. 204-211.

[3] J. Liu, P. Cuff and S. Verdú, "On α-decodability and α-likelihood decoder," // 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2017, pp. 118-124.

[4] J.-T. Huang and Y.-H. Kim, "Parallel Monte Carlo Markov Chain Decoding of Linear Codes," // 2023 IEEE International Symposium on Information Theory (ISIT), Taipei, Taiwan, 2023, pp. 2051-2056

[5] Ilya Dumer, “Recursive decoding of Reed-Muller codes”, // Proc. 37th Allerton Conf. on Commun., Control, and Computing, Monticello, IL, USA, 1999, pp. 61-69.

[6] Ипатов В.П. Широкополосные системы и кодовое разделение сигналов: принципы и приложения. М.: Техносфера, 2007. 488 с.