УДК 621.391

А.А. Кузнецов[1], С.И. Приходько[2], С.А. Гусев[2], В.А. Зубенко[3]

[1] *Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2] *Украинская государственная академия железнодорожного транспорта, Харьков*
[3] *Кировоградский национальный технический университет, Кировоград*

МЯГКОЕ ДЕКОДИРОВАНИЕ КАСКАДНЫХ КОДОВ-ПРОИЗВЕДЕНИЙ С ИСПОЛЬЗОВАНИЕМ УПОРЯДОЧЕННЫХ ПОДМНОЖЕСТВ ПРОВЕРОЧНЫХ УРАВНЕНИЙ

Рассматриваются методы мягкого декодирования каскадных кодовых конструкций, построенных на основе схем-произведений линейных блоковых кодов (турбо-продуктивных кодов, Turbo Product Codes). Развивается подход, основанный на итеративном обмене мягкими решениями между составляющими каскадную конструкцию блоковыми кодами. В основе предлагаемого метода декодирования лежит использование упорядоченных подмножеств проверочных уравнений линейных блоковых кодов.

Ключевые слова: *мягкое декодирование, каскадные конструкции, итеративный обмен.*

Введение

Постановка проблемы в общем виде и анализ литературы. Проведенные исследования показали, что каскадные кодовые конструкции являются перспективным направлением развития теории помехоустойчивого кодирования, совершенствования методов и алгоритмов обеспечения требуемой помехоустойчивости передачи дискретных сообщений [1 – 5]. Наиболее перспективными представляются коды, образованные каскадированием линейных блоковых кодов с быстрыми алгоритмами мягкого декодирования и итеративным обменом полученных решений. В зарубежной литературе такие каскадные кодовые конструкции получили название турбо-продуктивных кодов или турбо-кодов-произведений (Turbo Product Codes) [3 – 5]. С одной стороны они позволяют реализовывать обмен мягкими решениями в итеративной многошаговой процедуре декодирования для обеспечения высокой энергетической эффективности помехоустойчивого кодирования, с другой – строить вычислительно эффективные схемы кодирования-декодирования как в программном, так и в аппаратном виде.

В данной статье предлагается усовершенствованный метод мягкого декодирования каскадных кодовых конструкций с итеративным обменом мягких решений, который отличается от известных методов ускоренной процедурой отбора проверочных уравнений с наиболее достоверными символами, что позволяет реализовать декодирование кодовых слов по критерию минимизации ошибочного приема символов и ускорить процесс турбо-декодирования каскадных кодов.

Результаты исследований

Теоретическое обоснование предлагаемого метода декодирования. Теоретическую основу методов мягкого декодирования составляет критерий проверки гипотез, математическое обоснование которого основано на формуле полной вероятности и теореме Байеса [6, 7].

Предположим, что об обстановке опыта можно сделать M исключающих друг друга предположений (гипотез) H_1, H_2, …, H_M и событие A может появиться только при одной из этих гипотез.

Тогда вероятность события A вычисляется по формуле полной вероятности:

$$P(A)=P(H_1)P(A|H_1)+P(H_2)P(A|H_2)+\ldots+$$
$$+P(H_M)P(A|H_M)=\sum_{i=1}^{M}P(H_i)P(A|H_i),$$

где $P(H_i)$ – вероятность гипотезы H_i; $P(A|H_i)$ – условная вероятность события A при этой гипотезе.

Если до опыта априорные вероятности гипотез были $P(H_i)$, $i=1,2,\ldots,M$, а в результате опыта появилось событие A, то апостериорные (послеопытные, при условии появления события A) вероятности гипотез вычисляются по формуле Байеса:

$$P(H_i|A)=\frac{P(H_i)P(A|H_i)}{\sum_{i=1}^{M}P(H_i)P(A|H_i)},\ i=1,2,\ldots,M.$$

Формула Байеса дает возможность вычислять условные вероятности появлений следующих за A событий с учетом апостериорных вероятностей гипотез $P(H_i|A)$, $i=1,2,\ldots,M$. Так, если после первого опыта, в котором появилось событие A, производится следующий опыт, в котором может появиться событие B, то условная вероятность $P(B|A)$ вычисляется по формуле полной вероятности, в которую подставлены не априорные вероятности $P(H_i)$, а апостериорные, вычисленные после наступления события A, вероятности $P(H_i|A)$, т.е. получим:

$$P(B|A)=\sum_{i=1}^{M}P(H_i|A)P(B|H_iA),\ i=1,2,\ldots,M,$$

где H_iA – событие A при гипотезе H_i, $P(B|H_iA)$ – условная вероятность события B при гипотезе H_i и событии A.

Предположим теперь, что демодулятор на основе наблюдения принятой смеси сигнала и помехи $S*$ оценивает, какой из возможных сигналов $S_i\in\{S_1,S_2,\ldots,S_M\}$, (из ансамбля сигналов мощностью M) был передан. Выдвинем M исключающих друг друга предположений (гипотез) о том, что передавался соответствующий сигнал S_i, $i=1,2,\ldots,M$. Вычислим апостериорную вероятность i-ой гипотезы, при условии приема $S*$:

$$P(S_i|S*)=\frac{P(S_i)P(S*|S_i)}{\sum_{i=1}^{M}P(S_i)P(S*|S_i)},\ i=1,2,\ldots,M, \quad (1)$$

где $P(S_i)$ – априорная вероятность формирования передатчиком сигнала S_i; $P(S*|S_i)$ – условная вероятность приема $S*$ при условии формирования передатчиком сигнала S_i.

Обычно $S*$ представляется непрерывной случайной величиной, лежащей в основе критерия проверки гипотез. Рассмотрим функцию $p(S*)$ распределения вероятностей $P(S*)=\sum_{i=1}^{M}P(S_i)P(S*|S_i)$.

$p(S*)$ – это функция распределения вероятностей смеси сигнала и помехи $S*$, дающая тестовую статистику в полном пространстве сигналов $\{S_1,S_2,\ldots,S_M\}$.

В уравнении (1) значение функции $p(S*)$ является коэффициентом масштабирования, поскольку величина $P(S*)$ получается путем усреднения по всему пространству сигналов.

Рассмотрим случай для двух сигналов. Пусть двоичные логические элементы 1 и 0 представляются сигналами $S_1=1$ и $S_2=-1$. На рис. 1. показана условная функция распределения вероятностей при передаче сигнала по каналу с аддитивным белым Гауссовым шумом (additive white Gaussian noise – AWGN), представленная как функция правдоподобия. Функция, изображенная справа, $P(S*|S_1)$, представляет функцию распределения вероятностей непрерывной случайной переменной $S*$, которая передается при условии, что принят сигнал S_1. Функция, изображенная слева, $P(S^*|S_2)$, в свою очередь, представляет ту же функцию распределения вероятностей непрерывной случайной переменной S^*, которая передается при условии, что принят сигнал S_2. На оси абсцисс показан полный диапазон возможных значений непрерывной случайной переменной S^*, которая образуется в приемнике.

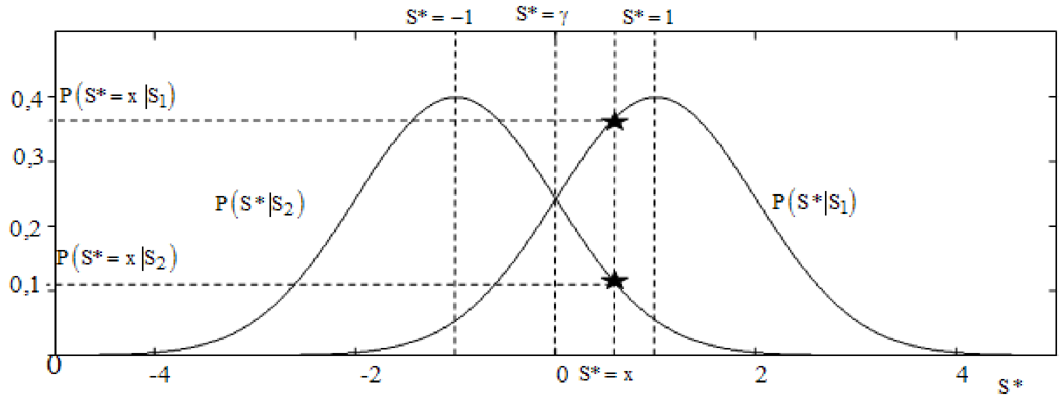

Рис. 1. Функции правдоподобия

Для примера на рис. 1 показано значение случайной переменной S^*. Прямая, опущенная в точку $S^* = x$, пересекает две кривые функций правдоподобия, что дает в итоге два значения апостериорной вероятности $P(S^* = x|S_1)$ и $P(S^* = x|S_2)$. Правило принятия решения по жесткой схеме, называемое как *правило максимального правдоподобия*, определяет выбор одной из гипотез (соответствующих передаче сигналов S_1 и S_2, соответственно) на основе сравнения значений вероятностей $P(S^* = x|S_1)$ и $P(S^* = x|S_2)$ и выборе большего из них. Для каждого переданного бита данных принимается решение о том, что передавался сигнал S_1, если $S^* = x$ попадает по правую сторону линии принятия решений (обозначенной γ), или что передавался сигнал S_2 в противном случае.

Аналогичное правило принятия решения, известное как *максимум апостериорной вероятности* (maximum a posteriori – MAP), можно представить в виде *правила минимальной вероятности ошибки,* принимая во внимание априорную вероятность данных. В общем случае правило MAP выражается следующим образом:

$$S = \begin{cases} S_1, \text{ если } P(S^* = x|S_1) > P(S^* = x|S_2) \\ S_2, \text{ если } P(S^* = x|S_1) < P(S^* = x|S_2) \end{cases}, \quad (2)$$

где S – значение сигнала, соответствующее принимаемому решению.

Таким образом, выражение (2) устанавливает правило выбора одной из гипотез, соответствующих сигналам S_1 и S_2. Используя выражение (1) получим эквивалентное выражение:

$$S = \begin{cases} S_1, \text{ если } P(S_1)P(S^*|S_1) > P(S_2)P(S^*|S_2) \\ S_2, \text{ если } P(S_1)P(S^*|S_1) < P(S_2)P(S^*|S_2) \end{cases}, \quad (2)$$

где вероятность

$$P(S^*) = \sum_{i=1}^{M} P(S_i)P(S^*|S_i)$$

в обеих частях неравенства сокращена.

Используя (2) введем функцию F как отношение функций правдоподобия $P(S^* = x|S_1)$ и $P(S^* = x|S_2)$:

$$F = \frac{P(S_1)P(S^*|S_1)}{P(S_2)P(S^*|S_2)}, \quad (3)$$

тогда правило выбора одной из гипотез запишется в виде

$$S = \begin{cases} S_1, \text{ если } F > 1 \\ S_2, \text{ если } F < 1 \end{cases}. \quad (4)$$

Прологарифмируем выражение (3), получим:

$$\ln F = \ln\left(\frac{P(S_1)}{P(S_2)}\right) + \ln\left(\frac{P(S^*|S_1)}{P(S^*|S_2)}\right).$$

Таким образом, логарифм отношения функций правдоподобия $\ln F$ является вещественным представлением мягкого решения на входе декодера, причем первое слагаемое в правой части равенства является логарифмом отношений априорных вероятностей $P(S_1)$ и $P(S_2)$, обозначим его

$$L_S(S_1, S_2) = \ln\left(\frac{P(S_1)}{P(S_2)}\right),$$

а второе слагаемое – суть логарифм отношения апостериорных вероятностей $P(S^*|S_1)$ и $P(S^*|S_2)$:

$$L_{DS}(S_1, S_2) = \ln\left(\frac{P(S^*|S_1)}{P(S^*|S_2)}\right)$$

как результат канальных измерений в приемнике.

Т.о. логарифм отношения функций правдоподобия $L_{FS} = \ln F$ перепишем в виде

$$L_{FS}(S_1, S_2) = L_S(S_1, S_2) + L_{DS}(S_1, S_2). \quad (5)$$

Следует отметить, что для каналов AWGN логарифм функции правдоподобия как результат канальных измерений принятой смеси сигнала и шума S^* в приемнике будет иметь следующий вид:

$$L_{DS}(S_1,S_2) = \ln\left[\frac{P(S^*|S_1)}{P(S^*|S_2)}\right] =$$

$$= \ln\left[\frac{\frac{1}{\sigma\sqrt{2\pi}}\exp\left[-\frac{1}{2}\left(\frac{S^*-1}{\sigma}\right)^2\right]}{\frac{1}{\sigma\sqrt{2\pi}}\exp\left[-\frac{1}{2}\left(\frac{S^*+1}{\sigma}\right)^2\right]}\right] =$$

$$= -\frac{1}{2}\left(\frac{S^*-1}{\sigma}\right)^2 + \frac{1}{2}\left(\frac{S^*+1}{\sigma}\right)^2 = \frac{2}{\sigma^2}S^*.$$

Принимая во внимание соотношение

$$\frac{1}{\sigma^2} = \frac{2E_b}{N_0},$$

где E_b/N_0 – отношение энергии двоичного сигнала E_b к спектральной плотности мощности шума N_0, получим:

$$L_{DS}(S_1,S_2) = 4\cdot(E_b/N_0)\cdot S^*,$$

т.е. значение логарифма отношения апостериорных вероятностей $P(S^*|S_1)$ и $P(S^*|S_2)$ как результат канальных измерений в приемнике зависит исключительно от отношения «сигнал/шум» и значения принятой смеси сигнала и шума S^*.

Например, для уровня помехи с дисперсией $\sigma^2 = 1$ соответствующая зависимость функции правдоподобия приведена на рис. 1.

Значение $\sigma^2 = 1$ соответствует

$$\frac{E_b}{N_0} = \frac{1}{2} = -3\text{dB}$$

и логарифм функции правдоподобия как результат канальных измерений принятой смеси сигнала и шума S^* в приемнике будет иметь следующий вид:

$$L_{DS}(S_1,S_2) = 2\cdot S^*.$$

Выражения (2) – (4) получены только исходя из данных демодулятора. Применение кодов исправляющих ошибки приведет к повышению достоверности принятия решения. Предположим, как и прежде, что при передачи информации используется два сигнала ($S_1 = 1$ и $S_2 = -1$) и соответствующие им двоичные кодовые символы $C_1 = 1$ и $C_2 = 0$.

В [7] показано, что для систематических кодов мягкое решение на выходе декодера (в логарифмическом масштабе) о принятом символе записывается в виде выражения:

$$L_{FDK}(S_1,S_2,C_1,C_2) = L_{FS}(S_1,S_2) + L_{DK}(c_1,c_2), \quad (6)$$

где $L_{DK}(C_1,C_2)$ – логарифм отношения функций правдоподобия о принятом символе, полученный в результате декодирования.

Подставляя (5) в (6) получим:

$$\begin{gathered} L_{FDK}(S_1,S_2,C_1,C_2) = L_S(S_1,S_2) + \\ + L_{DS}(S_1,S_2) + L_{DK}(c_1,c_2) \end{gathered}, \quad (7)$$

т.е. мягкое решение на выходе декодера зависит от трех величин: $L_S(S_1,S_2)$ – логарифм отношения априорных вероятностей сигналов S_1 и S_2; $L_{DS}(S_1,S_2)$ – логарифм отношения апостериорных вероятностей сигналов S_1 и S_2 (результат канальных измерений) и $L_{DK}(C_1,C_2)$ – логарифм отношения функций правдоподобия двоичных кодовых символов C_1 и C_2 как результат декодирования.

Чтобы получить $L_{FDK}(S_1,S_2,C_1,C_2)$, нужно просуммировать отдельные вклады, поскольку все три компонента статистически независимы [7]. Мяг-кий выход декодера $L_{FDK}(S_1,S_2,C_1,C_2)$ является вещественным числом, обеспечивающим как само принятие жесткого решения, так и его надежность. Знак $L_{FDK}(S_1,S_2,C_1,C_2)$ задает жесткое решение, т.е.:

$$c_i = \begin{cases} C_1 = 1, \text{ если } L_{FDK}(S_1,S_2,c_1,c_2) > 0 \\ C_2 = 0, \text{ если } L_{FDK}(S_1,S_2,c_1,c_2) < 0 \end{cases}, \quad (8)$$

где c_i – значение i-го бита, соответствующее принимаемому решению.

Собственное значение $L_{FDK}(S_1,S_2,C_1,C_2)$ определяет надежность принимаемого решения.

Как правило, величина $L_{DK}(C_1,C_2)$ имеет тот же знак что и $L_{FDK}(S_1,S_2,C_1,C_2)$, что повышает, таким образом, надежность принимаемого решения.

Для статистически независимых величин x и y сумма двух логарифмических отношений правдоподобия $L(x)$ и $L(y)$ определяется следующим выражением:

$$L(x)[+]L(y) = L(x\oplus y) = \ln\left[\frac{e^{L(x)} + e^{L(y)}}{1 + e^{L(x)}e^{L(y)}}\right] \approx \quad (9)$$

$$\approx (-1)\times\text{sgn}[L(x)]\times\text{sgn}[L(y)]\times\min(|L(x)|,|L(y)|),$$

где функция $\text{sgn}[z]$ возвращает знак своего аргумента z, а знак "$\oplus$" применяется для обозначения суммы по модулю 2 данных, представленных двоичными цифрами. Знак $[+]$ используется для обозначения суммы логарифмов функций правдоподобия, который определяется как логарифм функции правдоподобия суммы по модулю 2 соответствующих аргументов.

Вывод уравнения (9) основан на следующих рассуждениях. Запишем логарифм отношения функций правдоподобия в виде:

$$L(x) = \ln\left[\frac{P(x=+1)}{P(x=-1)}\right] = \ln\left[\frac{P(x=+1)}{1-P(x=+1)}\right],$$

так что

$$e^{L(x)} = \left[\frac{P(x=+1)}{1-P(x=+1)}\right]$$

Выражая $P(x=+1)$, получаем следующее:

$$e^{L(x)} - e^{L(x)} \times P(x=+1) = P(x=+1),$$

$$e^{L(x)} = P(x=+1) \times \left[1+e^{L(x)}\right],$$

и

$$P(x=+1) = \frac{e^{L(x)}}{1+e^{L(x)}}.$$

Откуда видно, что

$$P(x=-1) = 1-P(x=+1) = 1-\frac{e^{L(x)}}{1+e^{L(x)}} = \frac{1}{1+e^{L(x)}}.$$

Пусть x и y – два статистически независимых бита данных, принимающих значения $C_1=1$ или $C_2=0$ и соответствующих сигналам $S_1=1$ или $S_2=-1$. При таком формате сложение (по модулю 2) x и y дает – 1, если x и y имеют одинаковое значение (оба равны +1 или – 1, одновременно), и + 1, если x и y имеют разные значения. Тогда

$$L(x\oplus y) = \ln\left[\frac{P(x\oplus y=1)}{P(x\oplus y=-1)}\right] =$$

$$= \ln\left[\frac{P(x=+1)\times P(y=-1)+[1-P(x=+1)]\ [1-P(y=-1)]}{P(x=+1)\times P(y=+1)+[1-P(x=+1)]\ [1-P(y=+1)]}\right].$$

Воспользовавшись введенными выше обозначениями, получим следующее:

$$L(x\oplus y) =$$

$$= \ln\left[\frac{\left(\frac{e^{L(x)}}{1+e^{L(x)}}\right)\left(\frac{1}{1+e^{L(y)}}\right)+\left(\frac{1}{1+e^{L(x)}}\right)\left(\frac{e^{L(y)}}{1+e^{L(y)}}\right)}{\left(\frac{e^{L(x)}}{1+e^{L(x)}}\right)\left(\frac{e^{L(y)}}{1+e^{L(y)}}\right)+\left(\frac{1}{1+e^{L(x)}}\right)\left(\frac{1}{1+e^{L(y)}}\right)}\right] =$$

$$= \ln\left[\frac{\left(\frac{e^{L(x)}+e^{L(y)}}{\left[1+e^{L(x)}\right]\ \left[1+e^{L(y)}\right]}\right)}{\frac{e^{L(x)}e^{L(y)}+1}{\left[1+e^{L(x)}\right]\ \left[1+e^{L(y)}\right]}}\right] = \ln\left[\frac{e^{L(x)}+e^{L(y)}}{e^{L(x)}e^{L(y)}+1}\right].$$

Выражение

$F_1(a,b) = (-1)\times \mathrm{sgn}[a]\times \mathrm{sgn}[b]\times \min(|a|,|b|)$

является аппроксимацией (рис. 2) выражения

$$F_2(a,b) = \ln\left[\frac{e^a+e^b}{e^a e^b+1}\right],$$

т.е. имеем:

$$L(x\oplus y) \approx (-1)\times \mathrm{sgn}[L(x)]\times \mathrm{sgn}[L(y)]\times$$
$$\times \min(|L(x)|,|L(y)|).$$

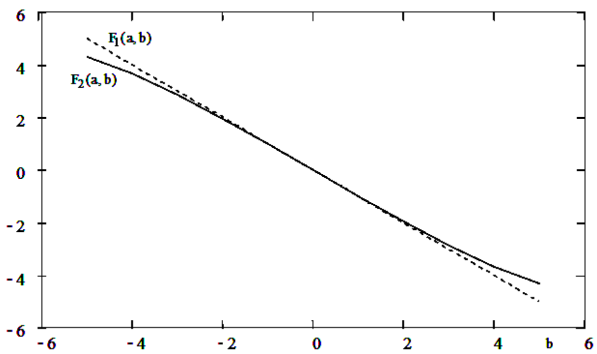

Рис. 2. График аппроксимации функции $F_2(a, b)$ функцией $F_1(a, b)$ для случая a = 5

Таким образом, выражение (9) аналитически задает одно из основных преобразований, используемых при реализации алгоритмов мягкого декодирования, – сложение логарифмов функции правдоподобия. Анализ соотношения (9) показывает, что имеют место равенства:

$$L(x)[+]\infty = -L(x),\ L(x)[+]0 = 0,$$

которые упрощают обработку вычислений над очень большими и очень малыми значениями логарифмов функции правдоподобия.

Реализация процедуры турбо-декодирования подразумевает использование методов декодирования с мягким решением на входе и мягким решением на выходе. Во время первой итерации на таком декодере, данные считаются равновероятными, что дает начальное априорное значение $L_S(S_1,S_2)=0$ в уравнении (7). Канальное измерение дает значение $L_{DS}(S_1,S_2)$, которое получается путем взятия логарифма отношения величин $P(S^*=x|S_1)$ и $P(S^*=x|S_2)$ для определенных значений x (рис. 1.) и является вторым членом уравнения (7). Выход декодера $L_{DK}(C_1,C_2)$ представляет собой сведения, вытекающие из процесса декодирования. Для итеративного декодирования внешнее правдоподобие подается обратно на вход (другого составного декодера) для обновления априорной вероятности информации следующей итерации, т.е. производится обновление априорной вероятности:

$$L_S(S_1,S_2) = L_{DK}(C_1,C_2).$$

Таким образом, решение при финальном декодировании каждого символа кодовой последовательности и сведения о его надежности зависят от величины $L_{FDK}(S_1,S_2,C_1,C_2)$. Основываясь на уравнении (7) запишем алгоритм, дающий оценку мягкого выхода декодера $L_{DK}(C_1,C_2)$ и результирующую оценку $L_{FDK}(S_1,S_2,C_1,C_2)$.

1. Устанавливаем $L_S(S_1,S_2)=0$.

2. Декодируем с мягким решением первый составной код, т.е. находим мягкое решение $L_{FDK}(S_1, S_2, C_1, C_2)$.

3. На основании уравнения (7) вычисляем $L_{DK}(C_1, C_2) = L_{FDK}(S_1, S_2, C_1, C_2) - L_S(S_1, S_2) - L_{DS}(S_1, S_2)$.

4. Для следующего составного кода устанавливаем $L_S(S_1, S_2) = L_{DK}(C_1, C_2)$.

5. Декодируем с мягким решением следующий составной код, т.е. находим мягкое решение $L_{FDK}(S_1, S_2, C_1, C_2)$.

6. Для всех составных кодов повторяем шаги 3 – 5.

7. Результатом турбодекодирования является жесткое решение о кодовом символе c по выражению (8) на основании полученного на последнем шаге мягкого решения $L_{FDK}(S_1, S_2, C_1, C_2)$.

Таким образом, как показывает анализ приведенного алгоритма, основной задачей при реализации турбодекодирования является разработка эффективных процедур мягкого декодирования составных кодов, т.е. разработка процедур вычисления мягкого решения $L_{DK}(C_1, C_2)$ для итеративной процедуры обмена в процессе турбодекодирования.

Исследуем процедуры нахождения мягкого решения $L_{DK}(C_1, C_2)$ на выходе декодера, проанализируем возможные пути вычисления последнего слагаемого в правой части равенства (7) – логарифма отношения функций правдоподобия двоичных кодовых символов C_1 и C_2 как результат декодирования.

Рассмотрим линейный блоковый $(n,\ k,\ d)$ код над конечным полем $GF(2)$. Линейный код, как подпространство $GF^k(2) \subseteq GF^n(2)$, задается порождающей матрицей G, строки которой образуют базис линейного пространства $GF^k(2)$. По определению, для каждого линейного кода существует ортогональное дополнение – подпространство $GF^{n-k}(2) \subseteq GF^n(2)$, все элементы которого ортогональны элементам из $GF^k(2)$.

Базис линейного пространства $GF^{n-k}(2)$ задается проверочной матрицей H, причем из условия взаимной ортогональности следует равенство $GH^T = 0$, где под «0» понимается $k \times r$ матрица нулевых элементов $GF(2)$.

Последнее равенство запишем в виде $cH^T = 0$, где $c = (c_0, c_1, ..., c_{n-1})$ – произвольное кодовое слово рассматриваемого линейного блокового $(n,\ k,\ d)$ кода, т.е. $c \in GF^k(2)$, $c_i \in [0,1]$.

Принимая во внимание тот факт, что все элементы $GF^{n-k}(2)$ могут быть выражены через линейную комбинацию строк проверочной матрицы H имеем: $ch_i^T = 0$, где $h_i = \left(h_{i_0}, h_{i_1}, ..., h_{i_{n-1}}\right)$ – произвольный вектор, полученный линейной комбинацией строк матрицы H, $i = 0,1,...,2^{n-k} - 1$.

Другими словами, последнее равенство выполняется для всех 2^{n-k} векторов из $GF^{n-k}(q)$ и имеем систему проверочных уравнений:

$$\begin{cases} c_0 h_{0_0} + c_1 h_{0_1} + ... + c_0 h_{0_{n-1}} = 0; \\ c_0 h_{1_0} + c_1 h_{1_1} + ... + c_0 h_{1_{n-1}} = 0; \\ ... \\ c_0 h_{\left(2^{n-k}-1\right)_0} + c_1 h_{\left(2^{n-k}-1\right)_1} + ... \\ \qquad + c_0 h_{\left(2^{n-k}-1\right)_{n-1}} = 0. \end{cases} \tag{10}$$

Предположим теперь, что кодовое слово $c = (c_0, c_1, ..., c_{n-1})$ принимается по критерию максимума апостериорной вероятности, т.е. получены значения логарифмов отношения апостериорных вероятностей $P(S^*|S_1)$ и $P(S^*|S_2)$:

$$L_{DS}(\tilde{n}_j) = L_{DS}(S_1, S_2) = \ln\left(P(S^*|S_1) / P(S^*|S_2)\right)$$

о каждом кодовом символе c_j, $j = 0,1,...,n-1$ как результат канальных измерений соответствующих сигналов в приемнике.

Логарифмы отношений априорных вероятностей $P(S_1)$ и $P(S_2)$, соответствующие каждому из кодовых символов c_j, $j = 0,1,...,n-1$ обозначим

$$L_S(c_j) = L_S(S_1, S_2) = \ln\left(\frac{P(S_1)}{P(S_2)}\right).$$

Тогда, с учетом (7) и правила (9) для i-го проверочного уравнения имеем:

$$L_{DK_i}(c_j) =$$

$$= \begin{cases} \left(L_S(c_0) + L_{DS}(c_0)\right) h_{i_0} [+] \left(L_S(c_1) + L_{DS}(c_1)\right) \times \\ \times h_{i_1} [+] ... [+] \left(L_S(c_{j-1}) + L_{DS}(c_{j-1})\right) h_{i_{j-1}} [+] \\ [+] \left(L_S(c_{j+1}) + L_{DS}(c_{j+1})\right) h_{i_{j+1}} [+] ... [+] \\ [+] \left(L_S(c_{n-1}) + L_{DS}(c_{n-1})\right) h_{i_{n-1}} = \\ = \sum\limits_{\substack{l=0,\\ l\neq j}}^{n-1} \left(L_S(c_l) + L_{DS}(c_l)\right) h_{i_l}, \quad \text{åñëè} \ h_{i_j} = 1; \\ \left(L_S(c_0) + L_{DS}(c_0)\right) h_{i_0} [+] \left(L_S(c_1) + L_{DS}(c_1)\right) \times \\ \times h_{i_1} [+] ... [+] \left(L_S(c_{n-1}) + L_{DS}(c_{n-1})\right) h_{i_{n-1}} = \\ = \sum\limits_{l=0}^{n-1} \left(L_S(c_l) + L_{DS}(c_l)\right) h_{i_l}, \quad \text{åñëè} \ h_{i_j} = 0, \end{cases} \tag{11}$$

где суммирование «$[+]$» и «$\sum$ » ведется по правилу сложения логарифмов правдоподобия, т.е. по выражению (9).

Если предположить, что все оценки $L_{DK_i}(c_j)$, $j = 0,1,...,n-1$ статистически независимы (например, при взаимной ортогональности проверочных уравнений), то результирующая оценка $L_{DK}(c_j)$ запишется в виде:

$$L_{DK}(c_j) = \sum_{i=0}^{2^{n-k}-1} L_{DK_i}(c_j), \tag{12}$$

где суммирование производится по обычному арифметическому правилу сложения вещественных чисел.

Мягкий выход декодера

$$L_{FDK}(c_j) = L_{FDK}(S_1, S_2, C_1, C_2)$$

является вещественным числом, и определяется по выражению (7):

$$\begin{aligned} L_{FDK}(\tilde{n}_j) &= L_S(\tilde{n}_j) + L_{DS}(\tilde{n}_j) + L_{DK}(c_j) = \\ &= L_S(\tilde{n}_j) + L_{DS}(\tilde{n}_j) + \sum_{i=0}^{2^{n-k}-1} L_{DK_i}(c_j). \end{aligned} \tag{13}$$

Знак $L_{FDK}(c_j)$ задает жесткое решение по правилу (8):

$$\tilde{n}_j = \begin{cases} \tilde{N}_1 = 1, \ \text{åñëè} \ L_{FDK}(\tilde{n}_j) > 0; \\ \tilde{N}_2 = 0, \ \text{åñëè} \ L_{FDK}(\tilde{n}_j) < 0. \end{cases}$$

Выражения (11), (12) и (13) задают решающую функцию, основанную на использовании логарифмов отношения функций правдоподобия принимаемых сигналов (вычисленных с использованием априорных и апостериорных вероятностей), а так же логарифма отношения функций правдоподобия двоичных кодовых символов в результате декодирования. Соответствующая сумма (12) задает решающую функцию, основанную только на использовании результата декодирования.

Проанализируем выражение (12). Раскрывая знак суммирования по правилу (11) получим, что выражение (12) содержит 2^{n-k} слагаемых, каждое из которых результат суммирования n логарифмов правдоподобия кодовых символов. В свою очередь, логарифмы правдоподобия кодовых символов – суть сумма логарифмов правдоподобия принимаемых сигналов (вычисленных с использованием априорных и апостериорных вероятностей). Очевидно, что с увеличением кодовых (n, k, d) параметров число слагаемых быстро возрастает и уже при $n-k > 32$ применение рассмотренного подхода становиться вычислительно нецелесообразным. Перспективным направлением в этом смысле является разработка правила формирования упорядоченных подмножеств проверочных уравнений и теоретическое обоснование на их основе решающих функций для методов декодирования с мягкими решениями.

Формирование упорядоченных подмножеств проверочных уравнений для мягкого декодирования линейных блоковых кодов. Для разработки правила формирования упорядоченных подмножеств проверочных уравнений рассмотрим процесс вычисления мягкого решения на выходе декодера $L_{FDK}(c_j)$:

$$L_{FDK}(c_j) = L_S(c_j) + L_{DS}(c_j) + \sum_{i=0}^{2^{n-k}-1} L_{DK_i}(c_j).$$

Предположим, что для всех $i = 0,1,...,2^{n-k}-1$ соответствующие $h_{i_j} = 0$. Тогда после подстановки выражения (11) получим:

$$\begin{aligned} L_{FDK}(\tilde{n}_j) &= L_S(\tilde{n}_j) + L_{DS}(\tilde{n}_j) + \\ &+ \sum_{\substack{i=0, \\ h_{i_j}=0}}^{2^{n-k}-1} \sum_{l=0}^{n-1} \left(L_S(c_l) + L_{DS}(c_l)\right) h_{i_l}, \end{aligned} \tag{14}$$

где первый знак суммирования в последнем слагаемом в правой части выражения соответствует обычному арифметическому сложению, второй знак суммирования соответствует сложению логарифмов по выражению (9).

Предположим, что $L_S(c_j) = 0$ (т.е. выполняется первая итерация турбодекодирования). Подставив (9) в (14) и произведя несложные преобразования, получим:

$$\begin{aligned} L_{FDK}(\tilde{n}_j) &= L_S(\tilde{n}_j) + L_{DS}(\tilde{n}_j) + \\ &+ \sum_{\substack{i=0, \\ h_{i_j}=0}}^{2^{n-k}-1} \sum_{l=0}^{n-1} \left(L_S(c_l) + L_{DS}(c_l)\right) h_{i_l} = \\ &= L_{DS}(\tilde{n}_j) + \sum_{\substack{i=0, \\ h_{i_j}=0}}^{2^{n-k}-1} (-1)^{|h_i|} \min_{l=0,..,n-1} \left(\left|L_{DS}(c_l)\right|\right) h_{i_l}, \end{aligned}$$

где $|h_i|$ – число ненулевых элементов в векторе $h_i = (h_{i_0}, h_{i_1}, ..., h_{i_{n-1}})$.

Анализ последнего выражения показывает, что при независимом искажении кодовых символов c_j и c_l, $l = 0,1,...,n-1$ соответствующая оценка $L_{DK}(c_j)$ при $L_S(c_j) = 0$ будет близка к нулю (значения слагаемых в правой части равенства «компенсируют» друг друга), что практически означает малый вклад проверочных уравнений с соответствующими $h_{i_j} = 0$ в результирующую оценку $L_{FDK}(c_j)$.

Предположим теперь, что $L_S(c_j) \neq 0$, а знак $L_S(c_j)$ и знак $L_{DS}(c_j)$ совпадают (это наиболее вероятное предположение, поскольку $L_S(c_j)$ вычисляется из $L_{DS}(c_j)$ на предыдущем шаге декодирования). Подставив (9) в (14) и произведя несложные преобразования, получим:

$$L_{FDK}(\tilde{n}_j) = L_S(\tilde{n}_j) + L_{DS}(\tilde{n}_j) + \sum_{\substack{i=0,\\ h_{i_j}=0}}^{2^{n-k}-1} \sum_{l=0}^{n-1} \left(L_S(c_j) + L_{DS}(c_l)\right) h_{i_l} =$$

$$= L_{DS}(\tilde{n}_j) + L_{DS}(\tilde{n}_j) + \sum_{\substack{i=0,\\ h_{i_j}=0}}^{2^{n-k}-1} (-1)^{|h_i|} \min_{l=0,..,n-1} \left(\left|L_S(c_j) + L_{DS}(c_l)\right|\right) h_{i_l},$$

что также дает близкое к нулю значение $L_{DK}(c_j)$.

Другими словами, при $h_{i_j} = 0$ и любом $L_S(c_j)$ соответствующие оценки $L_{DK}(c_j)$ будут близки к нулю и вносят, таким образом, малый вклад в результирующую оценку $L_{FDK}(c_j)$.

В данной работе предлагается использовать упорядоченное подмножество проверочных уравнений:

$$I_h = \begin{cases} c_0 h_{i0_0} + c_1 h_{i0_1} + \ldots + c_j h_{i0_j} + \ldots + c_0 h_{i0_{n-1}} = 0; \\ c_0 h_{i1_0} + c_1 h_{i1_1} + \ldots + c_j h_{i1_j} + \ldots + c_0 h_{i1_{n-1}} = 0; \\ \ldots \\ c_0 h_{(iM-1)_0} + c_1 h_{(iM-1)_1} + \ldots + c_j h_{(iM-1)_j} + \ldots \\ \qquad + c_0 h_{(iM-1)_{n-1}} = 0, \end{cases} \quad (15)$$

где $i0$, $i1$, …, $iM-1$ такие номера проверочных уравнений из системы (10), для которых соответствующие $h_{i_j} \neq 0$.

Очевидно, что число уравнений в системе (15) значительно меньше 2^{n-k}, т.е. $M << 2^{n-k}$, что с одной стороны, значительно упрощает реализацию соответствующего алгоритма декодирования. С другой стороны, предварительно упорядочивание уравнений в системе (15) позволяет повысить достоверность принимаемого решения. Рассмотрим процедуру упорядочивания подробнее.

Как было показано выше значение логарифма отношения правдоподобия $L_{DS}(c_j)$ как результат канальных измерений приемником $L_{DS}(S_1, S_2)$ можно записать в виде

$$L_{DS}(\tilde{n}_j) = L_{DS}(S_1, S_2) = 4 \cdot (E_b / N_0) \cdot S^*,$$

где $(E_b / N_0) = 1 / (2\sigma^2)$ – отношение энергии двоичного сигнала E_b к спектральной плотности мощности шума N_0, σ^2 – дисперсия помехи в канале AWGN.

Принимая во внимание (4) имеем, что при правильном принятии решения в «идеальном» случае $L_{DS}(c_j) = \pm 4 \cdot \frac{E_b}{N_0} = \pm F(E/N)$, что дает возможность упорядочить уравнения в системе (15).

Введем для каждого проверочного уравнения из (15) следующую оценку:

$$F_i = \frac{1}{|h_i|} \sum_{l=0}^{n-1} \left| L_{DS}(c_l) h_{i_l} \right|, \; i = i0, i1, \ldots, iM-1, \quad (16)$$

как среднюю величину абсолютных значений логарифмов отношения правдоподобия $L_{DS}(c_l)$, соответствующих ненулевым элементам проверочных уравнений.

Очевидно, что в «идеальном» случае $F_i = \left| L_{DS}(c_j) \right|$. Помехи в канале связи изменяют величины $L_{DS}(c_l)$ в (16) и могут как уменьшить (в случае несовпадения знака помехи и сигнала) так и увеличить (в случае совпадения знака помехи и сигнала) абсолютные значения $\left| L_{DS}(c_l) \right|$. Оценка F_i дает среднее значение $\left| L_{DS}(c_l) \right|$ по всем элементам кодового слова, принимающими участие в оценке $L_{DS}(c_j)$. Проверочные уравнения с большим F_i дают, таким образом, более достоверную оценку $L_{DK_i}(c_j)$, вычисленную по правилу (11), которое в данном случае запишется в виде

$$L_{DK_i}(c_j) = \sum_{\substack{l=0,\\ l \neq j}}^{n-1} \left(L_S(c_l) + L_{DS}(c_l)\right) h_{i_l}. \quad (17)$$

Полученные по выражению (16) оценки средней величины абсолютных значений $L_{DS}(c_l)$, $l = 0, 1, \ldots, n-1$ будем использовать в качестве весовых коэффициентов в уравнении (12) при оценке логарифма правдоподобия $L_{DK}(c_j)$, т.е. выражение (12) перепишется в виде

$$L_{DK}(c_j) = \sum_{i=i0}^{iM-1} F_i L_{DK_i}(c_j). \quad (18)$$

Выражение (18) совместно с упорядоченным подмножеством проверочных уравнений (15) задают правило декодирования с мягкой оценкой принимаемых решений о достоверности кодовых символов $L_{DK}(c_j)$.

Мягкий выход декодера

$$L_{FDK}\left(c_j\right)=L_{FDK}\left(S_1,S_2,C_1,C_2\right)$$

с использованием формируемых упорядоченных подмножеств проверочных уравнений является вещественным числом, и определяется по выражению:

$$L_{FDK}\left(\tilde{n}_j\right)=L_S\left(\tilde{n}_j\right)+L_{DS}\left(\tilde{n}_j\right)+L_{DK}\left(c_j\right)= \\ =L_S\left(\tilde{n}_j\right)+L_{DS}\left(\tilde{n}_j\right)+\sum_{i=i0}^{iM-1}F_i L_{DK_i}\left(c_j\right). \quad (19)$$

Знак $L_{FDK}\left(c_j\right)$ как и прежде задает жесткое решение по правилу (8).

Следует отметить, что предложенное правило обобщает известный метод, основанный на использовании пороговых схем. Так, если предположить, что в качестве линейного блокового кода используется допускающий полную ортогонализацию (в смысле разбиения множества проверочных уравнений на подмножества, во все из которых входит сомножитель при ненулевом h_{i_1}, а все остальные элементы проверочных уравнений входят только один раз) код, выражение (18) с $\forall i: F_i=1$ и множество проверочных уравнений (15) полностью будут соответствовать известному правилу принятия решения в пороговых схемах мягкого декодирования [7]. Сходимость в этом крайнем случае с известными положениями теории помехоустойчивого кодирования подтверждает достоверность и адекватность полученных результатов.

Выводы

В результате проведенных исследований усовершенствован метод мягкого декодирования каскадных кодовых конструкций с итеративным обменом мягких решений, который отличается от известных методов ускоренной процедурой отбора проверочных уравнений с наиболее достоверными символами, что позволяет реализовать декодирование кодовых слов по критерию минимизации ошибочного приема кодовых символов и ускорить процесс турбо-декодирования каскадных кодов. Предложена ускоренная процедура отбора проверочных уравнений с наиболее достоверными символами. Формируемые оценки средней величины абсолютных значений логарифмов отношения правдоподобия кодовых символов используются в качестве весовых коэффициентов проверочных уравнений. Это позволяет в ходе декодирования адаптивно учитывать достоверность принятых символов.

Перспективным направлением дальнейших исследований является экспериментальная проверка эффективности предложенных методов декодирования, оценка достигаемого энергетического выигрыша от турбо-продуктивного кодирования при использовании итеративного обмена мягкими решениями и упорядоченных подмножеств проверочных уравнений линейных блоковых кодов.

Список литературы

1. *Berrou C. Near Shannon Limit Error- Correcting Coding and Decoding: Turbo Codes / C. Berrou, A. Glavieu , P. Thitimajshima // Proc. of the Intern. Conf. on Commun. – 1993. May. – P. 1064-1070.*
2. *MacKay D.J.C. Near Shannon limit performance of low density parity check codes / D.J.C. MacKay, R.M. Neal // IEEE Electronics Letters. – 1996. – V.32, №18. – P. 1645-1646.*
3. *Turbo Product Code Encoder / Decoder [Электронный ресурс]. – Режим доступа: at www.aha.com.*
4. *IEEE 802.16 Broadband Wireless Access Working Group. Turbo Code Comparison (TCC v TPC) [Электронный ресурс]. – Режим доступа: http://ieee802.org/16.*
5. *Turbo Product Code FEC. Comtech EF Data Corp. [Электр. ресурс]. – Режим доступа: www.comtechefdata.com.*
6. *Мак-Вильямс Ф.Дж Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Слоэн Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.*
7. *Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.*

Поступила в редколлегию 20.04.2011

Рецензент: д-р техн. наук, проф. С.В. Листровой, Украинская государственная академия железнодорожного транспорта, Харьков.

М'ЯКЕ ДЕКОДУВАННЯ КАСКАДНИХ КОДІВ-ДОБУТКІВ З ВИКОРИСТАННЯМ ВПОРЯДКОВАНИХ ПІДМНОЖИН ПЕРЕВІРОЧНИХ РІВНЯНЬ

О.О. Кузнецов, С.І. Приходько, С.А. Гусев, В.О. Зубенко

Розглядаються методи м'якого декодування каскадних кодових конструкцій, побудованих на основі схем-добутків лінійних блокових кодів (турбо-продуктивних кодів, Turbo Product Codes). Розвивається підхід, заснований на ітеративному обміні м'якими рішеннями між складаючими каскадну конструкцію блоковими кодами. У основі пропонованого методу декодування лежить використання впорядкованих підмножин перевірочних рівнянь лінійних блокових кодів.

Ключові слова: *м'яке декодування, каскадні конструкції, ітеративний обмін.*

SOFT DECODING OF CODES-WORKS OF CASCADES WITH THE USE OF WELL-ORGANIZED SUBSET OF VERIFICATIONS EQUALIZATIONS

A.A. Kuznetsov, S.I. Prihod'ko, S.A. Gusev, V.A. Zubenko

The methods of the soft decoding of constructions of codes of cascades, built on the basis of charts-works of linear codes of blocks are examined (Turbo Product Codes). Approach, based on a iterative exchange soft decisions between by constituents cascade construction by the codes of blocks, develops. The use of well-organized subset of verifications equalizations of linear codes of blocks lies in basis of the offered method of decoding.

Keywords: *soft decoding, cascade constructions, iterative exchange.*