УДК 621.394.147.3

Повышение эффективности перестановочных декодеров на базе когнитивных принципов

А.А. Гладких[,2], Т.Н. Масленникова[1], Н.А. Пчелин[1], А.И. Муракаев[1]

[1]ФНПЦ АО «НПО «Марс»

[2]ФГБОУ ВО Ульяновский государственный технический университет

Введение

К наиболее эффективным методам обеспечения высокого качества цифровой передачи в условиях высокого уровня шума канала относятся уже весьма мощные в настоящее время алгоритмы декодирования корректирующих кодов, в разработке которых теория помехоустойчивого кодирования, несомненно, имеет очень значительные успехи. Несмотря на высокие темпы прогресса цифровой обработки сигнала, проблема борьбы с помехами в канале связи остается актуальной. Система связи, не имеющая помехоустойчивого кодирования, по современным меркам считается малоэффективной и экономически не рентабельной.

Практика эксплуатации каналов связи с различной физической природой распространения сигнала показала, что подавляющее большинство таких каналов в большей или меньшей мере подвержены влиянию деструктивных факторов. Доказано, что для любого класса кодов предпочтительна схема мягкого декодирования, при которой декодер использует сведения о процедуре демодуляции символов, которые выражаются в виде вещественных чисел, получивших название мягких решений символов (МРС) или оценок надежности символов. В асимптотике декодеры подобного класса обеспечивают энергетический выигрыш кода до 3 дБ. Реализация подобных декодеров неизбежно приводит к применению сложных алгоритмов. В докладе рассматривается метод мягкого перестановочного декодирования систематических блоковых кодов с использованием МРС в формате целочисленных значений [1, 2].

Применение ранговой метрики к блоковым кодам

Большинство современных исследований в области теории связи ориентированы на развитие подвижной высокоскоростной связи. Реализация многих программ в этой области основывается на современной теории помехоустойчивого кодирования, в том числе на современной теории каскадных кодов с итеративно-алгебраическим декодированием. Подобный подход классифицируется как мягкий метод декодирования, палитра алгоритмов которого гораздо богаче, чем перечень возможных методов жесткой обработки информации. Очевидно, что роль декодера в общем тракте звена передачи информации возрастает, а роль каналов обратной связи от функции запросов и повторений искаженной информации сводится в большей степени к управлению сетевыми ресурсами. Действительно, в высокоскоростных сетях использование каналов обратной связи снижает эффективность применения сетевых компонентов и в перспективе системы с запросом и повторением целесообразно использовать в исключительных ситуациях.

Повышение эффективности работы мягкого декодера возможно на основе выбора нехэмминговых метрик. К таким подходам следует отнести методы списочного декодирования на основе разбиения множества разрешенных кодовых комбинаций на группы (кластеры), имеющих определённые признаки [1]. Однако, для подобного подхода не выработаны граничные оценки, хотя бы на основе аналитических моделей.

Для повышения корректирующей способности двоичных блоковых кодов в алгоритме работы декодеров подобных кодов предлагается использовать принцип упорядочения статистики, которая использует механизм МРС в порядке их убывания (возрастания). Это позволяет реализовать процедуру декодирования принятого приемником кодового вектора с использованием принципа образования эквивалентного кода из исходного кода, применяемого в системе связи [1]. Такое решение классифицируется как мягкое декодирование. Исследования в данной предметной области показывают, что мягкие декодеры по принципам своей работы можно разбить на три основных класса:

– декодеры с исправлениями стираний;

– декодеры с разбиением пространства разрешенных кодовых комбинаций на кластеры;

– перестановочное декодеры с системой упорядочения МРС или оценок надежности.

Конструкция декодеров с исправлением стираний достаточно подробно описаны в работах [1, 3]. Асимптотические оценки подобных декодеров обеспечивают энергетический выигрыш, определяемый выражением $D_h = 10\lg(R(t+1))$ дБ. При реализации мягких декодеров подобные оценки в канале с гауссовским шумом при $E_b / N_0 \to \infty$ в случае жестких решений энергетический выигрыш оценивается выражением $D_s = 10\lg(Rd_{\min}) = 10\lg(R(2t+1))$ дБ [1]. В приведенных формулах: $R = k/n$ – скорость кода, а k – число информационных символов в кодовом векторе длины n, t – число, исправляемых кодом ошибок и $(d_{\min} = d)$ – метрика Хэмминга [1]. Отсюда следует, что при выполнении условия $E_b / N_0 \to \infty$ асимптотический выигрыш по энергетике при мягком декодировании примерно в два раза выше (на 3 дБ), чем при жестких решениях. В реальных системах связи подобная оценка справедлива при условии, что ошибочные символы совпадают с низкими значениями МРС. На практике из-за ложных решений по стираниям это выполняется с некоторой долей вероятности, как описано в работах [2, 3].

Метод разбиения пространства кодовых векторов на кластеры предложен и исследован в работе [2]. Его суть заключается в том, что источник информации, работая в поле элементов из $GF(2^k)$, где $\mathrm{k} \in \mathrm{N}$ – число разрядов в комбинации безызбыточного кода, после прохождения канального кодера, содержащего порождающую матрицу $G_{\mathrm{k \times n}}$, формирует на его выходе последовательности длины $n > k$. Этой операцией групповой код $C_{n,k}$ над полем элементов из $GF(2^n)$ считается заданным [2]. Исходя из свойств вложенности двоичных полей степени расширения n и менее, комбинации любого кода $C_{n,k}$ могут быть разбиты на кластеры с уникальными номерами ϕ_s и, следовательно, упорядочены лексикографически, где $1 \le \phi \le \mathrm{k}$ – число двоичных разрядов, определяющих номер кластера, а s – принятая система счисления [1]. Тогда $C_{n,k} = \{\{c_0\}, \{c_1\}, ..., \{c_{2^\phi - 1}\}\}$, где $\{c_i\}$ – множество комбинаций из $C_{n,k}$, принадлежащих кластеру с номером $\phi_s = i$, где $i = \overline{0, 2^\phi - 1}$ [1]. В новых условиях все комбинации кода содержат три непересекающихся между собой по символам кодового вектора части: $\langle \phi \rangle$ – сочетание любых произвольно выбранных разрядов кодовой комбинации, обозначающих номер ϕ_s кластера; $\langle k - \phi \rangle$ – любые разряды кодового вектора, представляющие индикатор эквивалентности кода; $\langle n - k \rangle$ – другие, не используемые в процедуре кластеризации и не обязательно избыточные разряды [2].

В случае списочного декодирования по кластерам необходимо получать надежные МРС, которые должны следовать подряд. На рисунке 2 представлена оценка подобных событий для кода Хэмминга (7,4,3) и некоторых кодов БЧХ. В ходе моделирования рассматривались различные размерности номера кластера и вероятность его восстановления по максимальным МРС. Увеличение символов в номере кластера, например, с двух до пяти, приводят к резкому снижению вероятности правильной идентификации номера кластера. Следовательно, целесообразна специфическая защита символов номера кластера, которая оказывается актуальной как для двоичной, так и для НДК. Заметно, что длина комбинации номера кластера меньше значения k. На рисунках 1 и 2 приведены результаты имитационного моделирования различных последовательностей двоичных символов, представляющих длины кодовых комбинаций наиболее характерные для использования в качестве внутренних кодов системы с каскадным кодированием. В ходе экспериментов учитывались только максимальные значения МРС. Это позволяет утверждать, что полученные результаты носят характер граничных оценок.

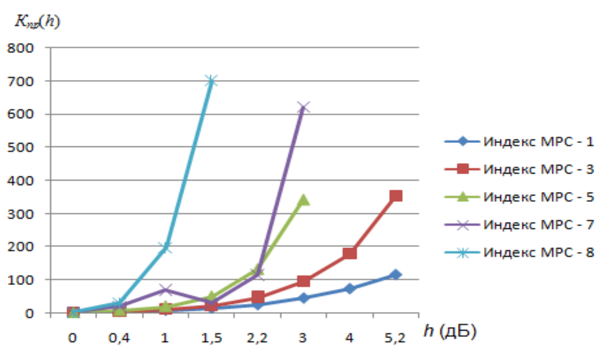

Рисунок 1 – Значение коэффициента правдоподобия

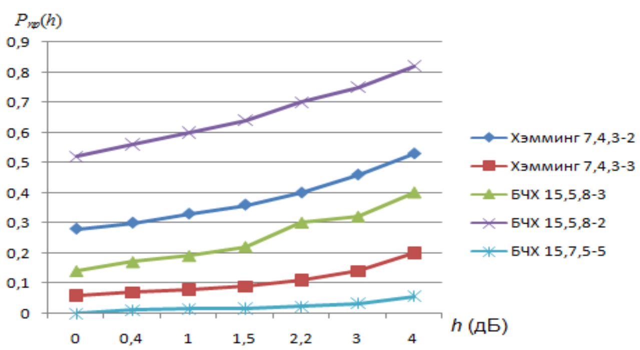

Рисунок 2 – Вероятность следования значений $\lambda_{\max}$ среди n_1 символов

Очевидно непрерывное следование максимальных значений МРС $\lambda_{\max}$ на длине кодового вектора накладывает серьезные ограничения на метод кластерного разбиения, поскольку вероятность встретить на отрезке символов длины n_1 подобные оценки в разбивку оболе вероятно. На основании этого можно утверждать о строгости неравенства вида $P_{перест} < P_{кластер}$, которое определяет вероятности появления ошибочных символов на бит при использовании той или иной технологии исправления мягких решений символов.

Окончательно можно утверждать, что в системах с исправлением стираний на основе МРС выполняется условие вида $P_{перест} < P_{кластер} < P_{мягк} < P_{алгебр}$.

Суть перестановочного декодирования заключается в том, что множество МРС зафиксированных на длине n_1 принятого вектора $V_{пр}$ $\{\lambda_j\}$, где $j = \overline{1, n_1}$, ранжируются по убыванию, например, $\{\hat{\lambda}\} = (\lambda_3 \geq \lambda_{n_1} \geq \lambda_6 \geq ... \geq \lambda_4)$, где $\lambda_3 = \lambda_{\max}$, а $\lambda_1 = \lambda_{\min}$. В переставленном векторе выбираются k левых разрядов с наиболее высокими значениями МРС (k – число информационных разрядов), которые с определенной вероятностью считаются принятыми верно. На основе указанной перестановки формируют матрицу перестановок P. С помощью коэффициента правдоподобия $K_{пр}(h) = N_{\lambda пр} / N_{\lambda ош}$, где $N_{\lambda пр}$ и $N_{\lambda ош}$ – соответственно частота появления правильных и ошибочных жестких решений с конкретным значением МРС можно оценить вероятность ошибочного декодирования. Как правило, $N_{\lambda пр}$ > $N_{\lambda ош}$, поэтому при относительно высоких отношениях сигнал-шум $K_{пр}(h)$ резко возрастает и при $h = 1$ правильные оценки на 2, 3 порядка превосходят ошибочные оценки такого же ранга, что повышает доверие к максимальным МРС.

Используя значения матрицы P, переставляют столбцы порождающей матрицы исходного кода G и приводят переставленную матрицу $\hat{G}$ к систематической форме. После чего умножают выбранные k элементов на $\hat{G}$, получая безошибочный вектор эквивалентного кода $V_{экв}$. Умножая его на P^T, получают вектор $V_{пром}$ и, выполняя $V_{пр} \oplus V_{пром} = E$, получают вектор ошибок, действовавший в канале связи. В работе предлагается на основе когнитивного принципа вырабатывать и запоминать значение P и соответствующее значение $\hat{G}$ и извлекать их из памяти в случае появления соответствующего набора

Обычно возможности кодов рассматриваются с точки зрения применения в декодере метрики Хэмминга. При этом целесообразно исправлять не ошибки, а стирания, кратность которых в два раза выше, чем кратность исправляемых кодом ошибок. Использование упорядоченной статистики при декодировании блоковых кодов позволяет повысить кратность исправляемых стираний до значения $n - k$, где n - общая длина кодовой комбинации, а k - число информационных разрядов. В работах [1, 2] доказывается, что повышение кратности исправляемых стираний не является экзотической задачей, а реализуется за счет использования в системе эквивалентных кодов и разделения символов кодовой комбинации на две группы. В первую группу собираются наиболее надежные символы, тогда как ко второй группе относятся наименее надежные символы.

На примере кода БЧХ (15;5;7) рассмотрим поэтапное выполнение алгоритма с оценкой сложности реализации выполняемых операций. Порождающая матрица кода в систематической форме имеет вид:

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Пусть на вход кодера поступает вектор вида 1 1 0 1 0. В результате умножения вектора на порождающую матрицу на выходе кодера формируется последовательность: 1 1 0 1 0 1 1 0 0 1 0 0 0 1 1. После передачи этой последовательности по каналу связи принимается вектор, в котором в соответствии с вероятностью ошибки на бит, характерной данному каналу связи, возможно появление ошибок. Пусть образец ошибок имеет вид $e = 010010001101110$. Заметно, что представленный объем ошибочных символов превосходит исправляющую способность кода по исправлению не только ошибок, но и стираний. Естественно, что жесткий декодер и традиционный мягкий декодер не в состоянии исправить возникшую в канале связи комбинацию ошибок. Докажем, что подобная комбинация может быть исправлена за счет применения в декодере эквивалентных кодов. В результате передачи кодового вектора по каналу связи и наложения на него вектора ошибок получаем последовательность вида $n_{np} = 100111101001101$.

Эта последовательность фиксируется жестким декодером. В мягком декодере каждому жесткому решению приписывается степень его надежности. Пусть оценки надежности символов выражаются целыми числами от 0 до 7, как показано в таблице 1. Представим вектор n_{np} вместе с такими оценками

Таблица 1 – Представление кодовой комбинации совместно с МРС

Порядковый номер символа	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Значения бит	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1
Оценки надежности	4	3	6	5	4	7	7	7	4	3	6	2	3	2	5

Упорядочим символы вектора n_{np} по убыванию оценок надежности. Результат работы декодера представим в таблице 2. Заметно, что на первых k позициях оказались наиболее надежные символы, значения которых будут использованы для создания эквивалентного кода.

Таблица 2 – Результат работы декодера по упорядочению символов статистики

Порядковый номер символа	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Значения бит	1	0	0	1	1	1	1	0	1	0	0	1	1	0	1
Оценки надежности	4	3	6	5	4	7	7	7	4	3	6	2	3	2	5
Новое расположение символов	6	7	8	3	11	4	15	1	5	9	2	10	13	12	14
Новый вектор	1	1	0	0	0	1	1	1	1	1	0	0	1	1	0

Для создания эквивалентного кода необходимо найти порождающую матрицу такого кода. Для этого, используя матрицу перехода, выполним умножение истинной порождающей матрицы G' на матрицу перехода G_{nep}. В соответствии с теорией матриц это обеспечит перестановку столбцов матрицы G'. В результате будет получена матрица вида:

$$G`` = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Перестановка столбцов может привести к потере нелинейной зависимости между строками матрицы. Поэтому из матрицы G'' выделяем новую матрицу размерности $k \times k$ и, используя признак равенства детерминанта данной матрицы нулю (признак линейной зависимости строк) или отсутствие такого равенства (признак линейной независимости), делаем вывод о линейной зависимости или независимости строк матрицы G''. Если линейная зависимость проявляется, то необходимо поменять местами столбцы с номерами k и $k + 1$.

Линейная зависимость проверяется с использованием детерминанта матрицы $k \times k$. Принципиально эта процедура легко программируется для процессора приемника, однако объем вычислений существенно увеличивается с ростом k. В приведенном примере матрица $k \times k$ имеет вид:

$$G_{kxk} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Поскольку $\det G_{k\times k} = 1$, то новую порождающую матрицу можно привести к систематической форме и алгоритм вычисления вектора помех продолжается.

Оценим максимальное число операций, необходимых для вычисления детерминанта квадратных матриц некоторой размерности. Полученные результаты сведем в таблицу 3. Рассмотрим матрицу размерности 2×2.

Число операций, необходимых для вычисления определителя такой матрицы составляет: две операции умножения и одна операция вычитания (обратное действие операции сложения).

$$det \begin{pmatrix} a & b \\ a_1 & b_1 \end{pmatrix} = a \cdot b_1 - a_1 \cdot b.$$

Современные процессоры тратят на операцию сложения до 2 нс, а на операцию умножения – до 180 нс. Т.к. в декодере осуществляется умножение единиц и нулей, будем считать, с некоторой долей условности, что на операцию умножения операндов будет тратиться тоже 2 нс. Таким образом, на вычисление указанного определителя будет потрачено порядка 6 нс.

Таблица 3 – Временные интервалы для оценки определителей

Размерность матрицы $k \times k$					
2×2	3×3	4×4	5×5	6×6	7×7
$6 \cdot 10^{-9}$с	$4.6 \cdot 10^{-8}$с	$2.2 \cdot 10^{-7}$с	$1.2 \cdot 10^{-6}$с	$7{,}0 \cdot 10^{-6}$с	$4{,}9 \cdot 10^{-5}$с

Вычислим порождающую матрицу нового кода в систематической форме. Известно, что произведение матрицы $G_{k\times k} = A$ на ее обратное отображение $G_{k\times k}{}^{-1} = A^{-1}$ обеспечивает получение единичной матрицы $E_{k\times k} = E$. Выполнив действие $G_{k\times k}{}^{-1} = E_{k\times k}/G_{k\times k}$, получим обратную матрицу, которая точно указывает на порядок сложения строк матрицы G′′ для получения порождающей матрицы в систематической форме.

$$\mathrm{A}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 \\ 1 & -2 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 1 \end{pmatrix}$$

Поскольку все действия декодер выполняет в двоичном поле, то в обратной матрице четные значения необходимо заменить на нули. Таким образом, для получения матрицы в систематической форме, необходимо четвертую строку матрицы G′′ взять как первую строку. Для получения второй строки необходимо сложить первую и вторую строку матрицы G′′. Для получения третьей строки необходимо сложить вторую, четвертую и пятую строки матрицы G′′. Аналогично, для получения четвертой строки с учетом свойств двоичного поля, требуется сложить все строки матрицы, исключив вторую строку. Для пятой строки требуется комбинация первой, второй и пятой строки матрицы G′′. Изложенная схема является математической основой для реализации процедуры получения эквивалентного кода. Исследования показали, что в обратной матрице могут появиться значения |3|. В этом случае соответствующая строка порождающей матрицы G′′ считается активной. В результате преобразований получим порождающую матрицу эквивалентного кода, которая после выполнения указанных преобразований примет вид

$$G_{\text{сис}}{}'' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Закодируем вектор 1 1 0 0 0 порождающей матрицы $G_{сис}{}''$. Учитывая то, что на месте информационных разрядов после указанных преобразований находятся надежные символы, получаем возможность формирования вектора, который не будет содержать ошибок. Этот вектор будет иметь вид 1 1 0 0 0 1 1 1 0 0 1 1 0 0 1.

Складывая этот вектор с трансформированным в соответствии с ранговой метрикой вектором, полученным из канала связи, получим вектор ошибок.

$$\begin{matrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$$

В таком представлении вектор ошибок не соответствует комбинации ошибок, действовавшей в канале связи в момент передачи кодового вектора по этому каналу. Для получения истинной комбинации ошибок необходимо данный вектор умножить на перестановочную матрицу вида, которая легко получается путем транспонирования исходной перестановочной матрицы, которая была получена за счет расстановки символов по убыванию градации надежностей. Выполнение операции представлено в таблице 4.

Таблица 4 – Результат работы декодера по обратному упорядочению символов статистики

Номера упорядоченных символов	6	7	8	3	11	4	15	1	5	9	2	10	13	12	14
Упорядоченное значение ошибок	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
Порядковый номер символа	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Расположение ошибок после обратной перестановки	0	1	0	0	1	0	0	0	1	1	0	1	1	1	0
Исходный вектор ошибок	0	1	0	0	1	0	0	0	1	1	0	1	1	1	0

Заметно, что после обратной перестановки символов вектора ошибок полученное расположение ошибок полностью соответствует исходному вектору ошибок. Аналитическое моделирование подобной системы для блокового кода (7.4.3) показало потенциальные возможности представленной системы. Результаты моделирования показаны на рисунке 3, где показана вероятность ошибки набит при использовании перестановочного метода и метода, работающего в рамках метрики Хэмминга. На рисунке 4 показаны сравнительные оценки вероятности ошибочной регистрации комбинации кода и соответствующей вероятности ошибки на бит.

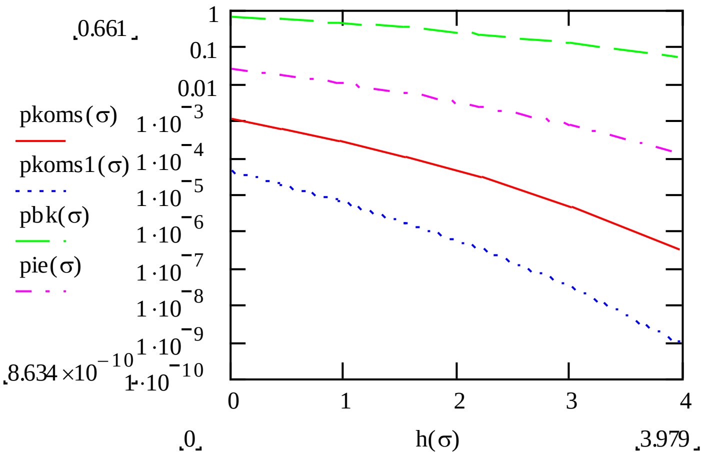

Рис. 3. Вероятность ошибки на комбинацию для кода (7.4.3)

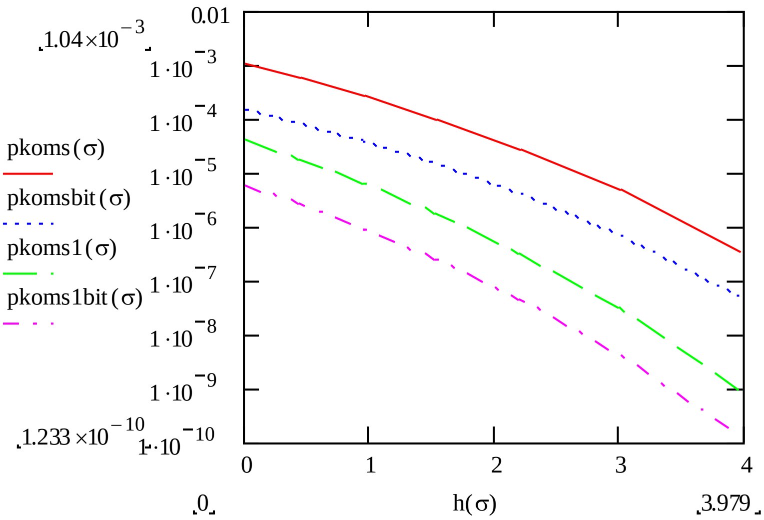

Рис. 4. Вероятность ошибки ин бит при использовании перестановочного декодирования

Заключение

Несомненно, перестановочное декодирование приближает характеристики двоичных кодов к характеристикам максимально декодируемых кодов. Наиболее трудоемкой операцией в вычислительном смысле для такого метода является операция проверки на четность переставленной порождающей матрицы и поиск ее систематического представления. Подобная задача должна решаться на пути реализации декодера с когнитивными функциями. В этом случае по мере накопления «опыта» работы декодер должен запоминать обработанные перестановки и хранить их в памяти. В случае повторения какой-либо перестановки вычисления не производятся, а соответствующая матрица извлекается из базы данных.

Литература

1. *Гладких, А.А.* Основы теории мягкого декодирования избыточных кодов в стирающем канале связи / А.А. Гладких. – Ульяновск : УлГТУ, 2010. – 379 с.
2. *Гладких, А.А.* Методы эффективного декодирования избыточных кодов и их современные приложения / А.А. Гладких, Р.В. Климов, Н.Ю. Чилихин. – УлГТУ, 2016. – 258 с.
3. *Березкин, А.А.* Введение в нейро-цифровые инфокоммуникационные технологии / А.А. Берёзкин, В.И. Комашинский // XI Санкт-Петербургская международная конференция «Региональная информатика-2008» (РИ-2008) : материалы / СПб. :, СПОАСУ 2008. С. 76.