МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
ВЫЧИСЛИТЕЛЬНЫХ МАШИН, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ

УДК 621.391.037

А.А. Гладких, Е.С. Бородина, Р.Ш. Шакуров

ДЕКОДИРОВАНИЕ НЕДВОИЧНЫХ КОДОВ В АДАПТИВНЫХ СИСТЕМАХ ОБМЕНА ДАННЫМИ

Гладких Анатолий Афанасьевич, *кандидат технических наук, окончил Военную академии связи им. С.М. Буденного, адъюнктуру этой академии, докторант Ульяновского государственного технического университета, доцент кафедры «Телекоммуникации» УлГТУ. Имеет монографию, учебные пособия, авторские свидетельства и научные статьи в области помехоустойчивого кодирования и защиты информации. [e-mail: a.gladfkikh@ulstu.ru].*

Бородина Екатерина Сергеевна, *аспирант кафедры «Телекоммуникации» УлГТУ, окончила Ульяновский государственный технический университет. Имеет публикации в области помехоустойчивого кодирования. [e-mail: bes_forever87@mail.ru].*

Шакуров Радик Шамильевич*, аспирант кафедры «Телекоммуникации» УлГТУ, окончил факультет автоматизированных систем управления войсками Ульяновского высшего военного инженерного училища связи. Имеет авторское свидетельство и публикации в области мягкого декодирования помехоустойчивых кодов [e-mail: ramazat@mail.ru].*

Аннотация

В статье представлено описание алгоритмов декодирования недвоичных помехоустойчивых кодов, используемых в адаптивных системах обмена информацией. Показано преимущество матричных вычислений для организации процедуры декодирования кодов Рида-Соломона относительно классических методов обработки таких кодов.

Ключевые слова: недвоичный код, мягкий декодер, помехоустойчивость, каскадный код, индекс достоверности символа, упорядоченная статистика.

Anatoly Afanasyevich Gladkikh*, Candidate of Engineering, graduated from the Military Communications Academy named after S. Budenny, finished his post-graduate studies of the same academy; doctoral student at Ulyanovsk State Technical University, Associate Professor at the Chair 'Telecommunications' at Ulyanovsk State Technical University; author of a monograph, text-books, research papers in the field of noise-immune coding and information security; has certificates of authorship in the same field. e-mail: a.gladfkikh@ulstu.ru.*

Ekaterina Sergeevna Borodina*, post-graduate student at the Chair 'Telecommunications' at Ulyanovsk State Technical University, graduated from Ulyanovsk State Technical University; author of publications in the field of noise-immune coding. e-mail: bes_forever87@mail.ru.*

Radik Shamilyevich Shakurov*, post-graduate student at the Chair 'Telecommunications' at Ulyanovsk State Technical University, graduated from the faculty of computer-aided systems for troop control at Ulyanovsk Higher Military Communications Engineering College; has a certificate of authorship and publications in the field of soft decoding of noise-immune codes. e-mail: ramazat@mail.ru.*

Abstract

The article gives a description of algorithms for decoding of non-binary noise-immune codes used in adaptive data-exchange systems, and shows advantages of matrix computations to organize a decoding procedure for Reed-Solomon codes over standard methods of processing of such codes.

Key words: non-binary code, soft decoder, noise immunity, cascade code, index of character reliability, ordered statistics.

Введение

Эффективность автоматизированных систем управления объектами во многом определяется качеством цифровой обработки информации в комплексах и системах связи. Повышение качества цифровой обработки информации сопряжено с постоянным усложнением алгоритмов, использованием методов, учитывающих изменяющиеся условия функционирования систем управления и систем связи в целом.

Увеличить скорость передачи информации при заданной помехоустойчивости или помехоустойчивость при постоянной скорости передачи в перспективных системах радиосвязи возможно за счет применения новых технологий помехоустойчивого кодирования, важным направлением которого является адаптивное кодирование. При этом следует учитывать, что основу многих современных систем управления составляют средства радиосвязи, главными недостатками которой являются: относительно высокий уровень помех при нестабильной динамике его изменения, ограниченность полосы пропускания, возникновение взаимных помех, работа в условиях высоковероятных организованных помех.

Обеспечение радиосвязи в наборе указанных факторов возможно при совершенствовании технических средств методов автоматизации и адаптации к изменяющимся характеристикам каналов связи.

1 Принцип декодирования двоичных кодов по упорядоченным статистикам

В современных системах обмена информацией принято различать три основных направления помехоустойчивого кодирования: блоковые коды, непрерывные и турбокоды. В свою очередь, турбокоды могут представлять собой композицию последовательно включенных блоковых кодов (каскадная схема кодирования) или сочетание параллельно включенных непрерывных кодеков. Исследования показывают, что наиболее эффективно адаптивные системы могут быть реализованы на основе блоковых кодов, поскольку применение сверточных кодов во многом сопряжено с реализацией структурной адаптации. Напротив, применение каскадных схем кодирования существенно расширяет спектр возможностей параметрической адаптации. В любом случае целесообразно использование мягких схем декодирования, основанных на упорядочивании индексов достоверности символов (ИДС) кодовой комбинации длины n по убыванию.

Пусть $Y = (y_1, y_2, \ldots, y_n)$ – упорядоченная последовательность ИДС, в которой $|y_1| \geq |y_2| \geq \ldots \geq |y_n|$. Реализация этой процедуры приводит к подстановке λ_1, такой, что $y = \lambda_1(r)$, где $r = (r_1, r_2, \ldots, r_n)$ – принятая последовательность символов. В ходе сортировки ИДС, отвечающих λ_1, создается перестановочная матрица R_{λ_1}. Следующий шаг декодирования состоит в перестановке столбцов порождающей матрицы $G = \left(I_{k\times k} \vdots H^T_{(n-k)\times k}\right)$ в систематической форме в порядке, соответствующем последовательности Y, здесь k – число информационных разрядов кода. Выполняя $G \times R_{\lambda_1}$, получим

$$G' = \lambda_1\left[G(Y)\right] = \left(g_1' g_2' \ldots g_n'\right),$$

где g_i' – i-й столбец матрицы G'. Естественно, образованная таким образом матрица G' на данном шаге алгоритма не является систематической [1].

Продолжение алгоритма состоит в построении наиболее надежного базиса возможного эквивалентного кода. Начиная с первого столбца матрицы G', находятся первые k линейно независимых столбцов, которым в соответствии с Y отвечают наибольшие ИДС. Остальные $(n - k)$ столбцов тоже упорядочиваются по убыванию их надежности, приводя к отображению λ_2, такому, что

$$G'' = \lambda_2\left[G'\right] = \lambda_2\left[\lambda_1\left[G(Y)\right]\right].$$

Применяя отображение λ_2 к последовательности Y, декодер получает новую переупорядоченную последовательность Z, где $Z = \lambda_2(Y) = (z_1, z_2, \ldots z_k, z_{k+1}, \ldots, z_n)$.

В этой последовательности $|z_1| \geq |z_2| \geq \ldots \geq |z_k| \geq |z_{k+1}| \geq \ldots \geq |z_n|$. Для проверки линейной независимости строк в матрице G' декодер выделяет первые k столбцов и, формируя квадратную матрицу $S_{k\times k}$, вычисляет ее детерминант. При $det\,(S_{k\times k}) \neq 0$, открывается возможность образования из матрицы G'' путем линейных преобразований ее строк и столбцов новой матрицы эквивалентного кода $G''_{сист}$ в систематической форме. Следует учитывать, что при $det\,(S_{k\times k}) = 0$ в матрице $S_{k\times k}$ наблюдается свойство линейной зависимости строк, что не позволяет сразу получить $G''_{сист}$. В случае линейной зависимости строк декодер переходит к итеративной процедуре преобразования $S_{k\times k}$ за счет смены мест столбцов с номерами k и $k + 1$ в G'. При отрицательном исходе первого шага итерации осуществляется смена мест столбцов с номерами $k + 1$ и $k + 2$ (второй шаг итерации). Выполнение последующих шагов итераций считается нецелесообразным, поскольку на позициях с номерами $k + 3$ и более с высокой вероятностью могут оказаться ошибочно принятые символы. В этом случае комбинация отмечается как стирание для последующего его восстановления на уровне внешних декодеров.

Получив удовлетворительный результат по вычислению $det(S_{k\times k})$, декодер должен выполнить регулярную процедуру по вычислению матрицы $G''_{сист}$. Известно, что произведение матрицы $S_{k\times k} = A$ на ее обратное отображение $A \times A^{-1} = E$ обеспечивает получение единичной матрицы. Исходя из этого, декодер выполняет стандартную процедуру вычисления такой матрицы и определяет обратную матрицу A^{-1}, которая точно указывает на порядок преобразования строк матрицы G'' для получения новой порождающей матрицы в систематической форме $G''_{сист}$.

Описанная процедура легко программируется для процессора приемника, однако следует учитывать, что объем вычислений экспоненциально увеличивается с ростом k. Для повышения скорости работы процессора приемника (сокращения объема вычислений) предлагается использовать принцип перехода от основного (n,k,d) кода к некоторому укороченному коду [2].

Таким образом, декодирование двоичных кодов по упорядоченным статистикам (УС) не всегда завершается полным использованием введенной в код избыточности и общая формула для оценки энергетического выигрыша от применения помехоустойчивого кода принимает вид:

$D = \mu_X \times 10lg(k(1-R+1/n)$, где $0 < \mu \le 1$ [3].

Заметно, что при $n = k$ (безызбыточное кодирование) $D = 0$. Здесь параметр μ_X определяет общее число удачных исходов в ходе анализа матрицы G'' на выполнение условий линейности. Оценка этого параметра для практически значимых кодов показывает, что значение μ_X колеблется от 0,75 до 0,8. Временные задержки при реализации указанной процедуры могут быть скомпенсированы повышением рабочей частоты процессора. Асимптотическая оценка метода указывает на возможность получения энергетического выигрыша до 2 дБ относительно мягких способов декодирования избыточных кодов.

2 Мягкое декодирование кодов Рида-Соломона

В системах турбокодирования с последовательным включением кодеров в качестве внешнего кода используют недвоичный код Рида-Соломона (РС). Внутренний двоичный код служит в этом случае индикатором обнаруженных ошибок.

Предположим, что для передачи сигналов по каналу с аддитивным белым гауссовым шумом (АБГШ) используется код РС (N,K) над полем $GF(2^m)$ с порождающей матрицей $G(x)$. Минимальное расстояние кода $d_{min} = N - K + 1 \ge 2t + 1$, где t – число исправляемых кодом ошибок. Порождающий полином $g(x)$ кода РС имеет степень $N - K = d_{min} - 1$.

Особенностью обработки недвоичных символов двоичного поля степени расширения m является повышенная сложность выполнения операции сложения относительно операции умножения по $mod\ 2$. При сложении двух символов в таком поле процессору необходимо обратиться к таблице сложения, найти первый и второй операнды и определить результат их сложения. Выполнение операции умножения осуществляется обычным сложением показателей степеней перемножаемых элементов по $mod\ (2^m - 1)$. Если значение параметра m мало, то действие с таблицей сложения не вызывает затруднений. При $m \ge 8$ таблица сложения должна содержать свыше 65 Кбайт памяти и выполнение операции сложения с помощью подобной таблицы занимает заметное время. Учитывая это, целесообразно оценивать сложность процедуры декодирования кодов РС по числу обращений к таблице сложения.

Пусть в поле $GF(q)$ существует элемент α^s, порядок которого $1 < l_s < q - 1$. Тогда совокупность элементов $1, \alpha^s, \alpha^{2s}, ..., \alpha^{(l_s-1)s}$ образует подгруппу, которая состоит из всех степеней одного из ее элементов, т. е. является циклической и совместно с нулевым элементом образует подполе поля $GF(q)$.

Значит, справедливо:

$$x^{l_s} - 1 = \prod_{i=1}^{l_s} \left(x - \alpha^{is}\right).$$

Таким образом, если в $GF(q)$ существует элемент a^s, порядок которого $1 < l_s < q - 1$, то возможно построение циклического кода РС над $GF(q)$ с длиной кодовой комбинации $N = l_s$ и порождающим многочленом:

$$g(x) = \prod_{i=1}^{D-1} \left(x - \alpha^{is}\right).$$

В системе с кодом РС искажение в одном разряде приводит к искажению символа кода РС. Тогда зависимость вероятности ошибочного приема кодовой комбинации кода РС определится по формуле:

$$p_{pc}(h) = \frac{1}{q} \sum_{i=t+1}^{q} i \cdot C_i^q \left(p(h)\right)^i \cdot \left(1 - p(h)\right)^{q-i},$$

где h – отношение сигнал-шум, измеряемое в дБ. Аналитическое моделирование системы с кодом РС в канале с АБГШ показывает, что наиболее предпочтительными являются характеристики укороченных кодов.

В классической схеме декодирования кодов РС обычно выделяют три основных этапа: этап первый – вычисление синдромов, требующий $2t(N - 1)$ обращений к таблице сложения; этап второй – вычисление локаторов ошибок с использованием алгоритма Берлекэмпа-Месси (АБМ), требующий около $t \cdot N$ обращений к таблице; и третий этап – решение ключевого уравнения Форни (по сути исправление ошибок), требующий около $6(N - 1)$ операций сложения. Общее число обращений к таблице сложения будет составлять

$$N_{\sum АБМ} = (2t + 6) \cdot (N - 1) + t \cdot N.$$

Оценим сложность декодирования комбинаций кода РС при использовании УС. Особенностью порождающей матрицы $G(x)$ размерности $N \times K$ в систематической форме такого кода является содержание первыми $N - K$ столбцами единственного элемента со значением $\alpha^0 = 1$. Указанное свойство может быть использовано для проверки надежности процедуры формирования $G(x)$ при моделировании систем с кодами РС.

Пусть от источника информации передается вектор $V_{ин}$ длины K. Кодирование вектора может осуществляться двумя способами: во-первых, с использованием регистра сдвига, отвечающего порождающему полиному $g(x)$; во-вторых, умножением вектора $V_{ин}$ на $G(x)$. При использовании укороченных кодов целесообразно применять второй метод. Таким образом, в канал связи будет отправлен вектор $V_{пер}$ длины N.

Приемник при обработке символов кода РС вырабатывает индексы достоверности для каждого символа. Допустим, при надежной фиксации недвоичного символа в результате его обработки внутренним кодом ему присваивается ИДС, равный λ_{max}. В случае существенного влияния на символ помех и высокой вероятности его неверного декодирования оценка символу присваивается λ_{min}.

Предположим, что приемная сторона приняла передаваемый вектор $V_{пер}$, в котором обнаружено t ошибок (принятый вектор $V_{пр}$). Процессор приемника присваивает достоверно принятым символам ИДС, равный λ_{max}, а сомнительным символам – ИДС, равный λ_{min}. При этом все символы со значением λ_{max} сортируются с начальных позиций вектора длины N, вытесняя символы со значением λ_{min} к концу вектора. На основе этого формируется матрица перестановок $R_{N\times N}$, которая отражает следующую последовательность действий. Декодер сортирует ИДС принятого вектора по убыванию так, что символы с высокой надежностью упорядочиваются слева, а символы с низкой надежностью собираются справа. В последующем надежные символы будут использованы для формирования эквивалентного кода.

Так, вектор после упорядочивания статистики $V_{ус}$ будет получен путем умножения принятого вектора $V_{пр}$ на перестановочную матрицу $R_{N\times N}$:

$$V_{ус} = V_{пр} \times R_{N\times N}.$$

Для получения эквивалентного кода РС необходимо преобразовать порождающую матрицу $G(x)$ в некоторую промежуточную матрицу $G(x)_{пром}$ в соответствии с данными матрицы перестановок:

$$G(x)_{пром} = G(x) \times R_{N\times N}.$$

Для получения порождающей матрицы эквивалентного кода РС $G(x)_{экв}$ из $G(x)_{пром}$ необходимо выделить квадратную матрицу Q размерности $K \times K$ и, используя стандартные функции, найти обратную матрицу $Q^{-1}_{K\times K}$. Матрица $Q^{-1}_{K\times K}$ отражает те преобразования, которые необходимо провести с матрицей $G(x)_{пром}$ для получения $G(x)_{экв}$ в систематической форме:

$$G(x)_{экв} = Q^{-1}_{K\times K} \times G(x)_{пром}.$$

Результатом кодирования информационной части вектора после упорядочивания статистики $V_{ус(инф)}$ будет эталонный вектор $V_{этал}$:

$$V_{этал} = V_{ус(инф)} \times G(x)_{экв}.$$

Чтобы получить переданный в канал связи вектор $V_{пер}$, нужно вектор $V_{этал}$ умножить на транспонированную перестановочную матрицу $R^{T}_{N\times N}$:

$$V_{этал} \times R^{T}_{N\times N} = V_{пер}.$$

Обработка информации перестановочными матрицами не требует выполнения операции сложения, поэтому общее количество обращений к таблице сложения оценивается в этом методе как:

$$N_{\sum ус} = K \times (N - K - 1).$$

Сравнительные данные для классического метода с применением АБМ направленного перебора в процедуре поиска корней полинома локатора ошибок и метода с применением УС приведены на рисунке.

Полученные данные свидетельствуют о целесообразности применения метода упорядоченной статистики для декодирования кодов РС. Особенностью метода является снижение вычислительных затрат с ростом кратности исправляемых ошибок. При использовании классического алгоритма с использованием процедуры подбора корней сложность алгоритма имеет тенденцию роста по мере увеличения кратности исправляемых ошибок. Поэтому классический алгоритм реально используется в системах с небольшой кратностью исправляемых ошибок. Подобный

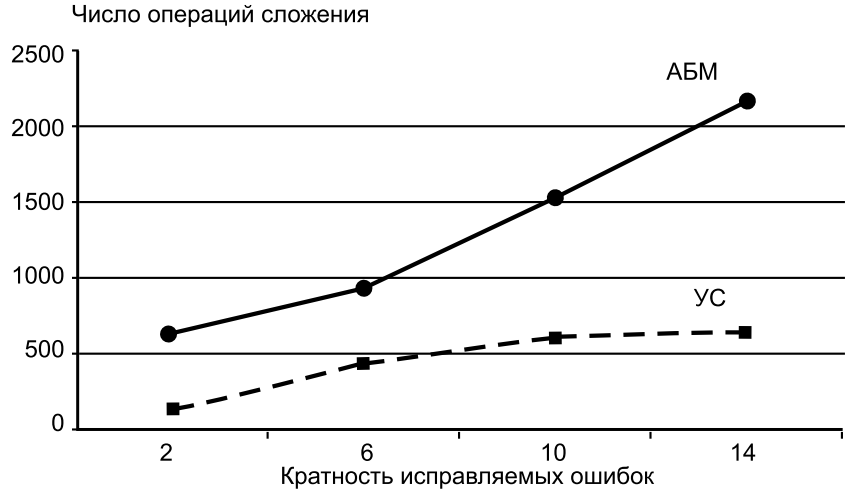

Рис. Сравнительная характеристика различных алгоритмов по числу обращений к таблице сложения

подход совершенно не пригоден для применения в системах связи с параметрической адаптацией. Предложенный в работе алгоритм исправления ошибок на основе упорядочения статистик свободен от указанного недостатка.

Выводы

Учитывая природу источника информации целесообразно код РС рассматривать над полем $GF(2^8)$, при этом следует использовать укороченный код как наиболее приспособленный к пакетной системе передачи информации.

При изменениях отношения сигнал-шум (или других параметров, которые могут быть пересчитаны в подобное отношение) целесообразно иметь несколько значений вводимой в код избыточности для оптимизации системы передачи данных по критерию скорости. При этом передатчик и приемник должны иметь списки порождающих полиномов кодов РС, в соответствии с которыми в ходе изменений условий передачи осуществляется синхронизация кодера (декодера) кода РС по порождающим полиномам. Значения внутреннего кода целесообразно не изменять.

СПИСОК ЛИТЕРАТУРЫ

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М. : Техносфера, 2005. – 320 с.

2. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи . – Ульяновск : УлГТУ, 2010. – 253 с.

3. Волков Л.Н, Немировский М.С., Шинаков Ю.С. Системы цифровой радиосвязи: базовые методы и характеристики : учеб. пособие. – М. : Эко-Трендз, 2005. – 392 с.