

Системы, сети и устройства телекоммуникаций

УДК 621.396

РАЗРАБОТКА АЛГОРИТМОВ ДИАГНОСТИКИ СВЕРТОЧНЫХ КОДОВ

Корнеева Наталья Николаевна

старший преподаватель кафедры радиотехники и радиосистем. ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».

E-mail: korneevanata@list.ru.

Никитин Олег Рафаилович

доктор технических наук, профессор, заведующий кафедрой радиотехники и радиосистем.

ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».

E-mail: olnikitin@mail.ru.

Полушин Петр Алексеевич

доктор технических наук, профессор кафедры радиотехники и радиосистем.

ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых».

E-mail: polushin.p@mail.ru.

Адрес: 600000, г. Владимир, ул. Горького, 87.

Аннотация: Рассмотрены и исследованы алгоритмы диагностики сверточных кодов. Определены их достоинства и недостатки. Рассмотрены пути практической реализации каждого из алгоритмов. На основе проведенного анализа выбран лучший алгоритм диагностирования сверточных кодов.

Ключевые слова: сверточное кодирование, помехоустойчивость передачи информации, «поисковые» полиномы, порождающие полиномы.

Постановка задачи

В настоящее время при передаче цифровых сигналов широко используется помехоустойчивое кодирование (FEC), которое дает возможность исправлять значительное число ошибок, возникающих в каналах передачи сигналов. Это возможно при внесении избыточных символов, определенным образом связанных с передаваемыми информационными символами. Закон, по которому формируются избыточные символы, и определяет используемый метод кодирования.

Применяется множество различных методов кодирования и их модификаций, однако почти все они относятся к одному из двух классов – к сверточному кодированию и к блочному кодированию ([1-5]). Для успешного декодирования и исправления ошибок на при-

емной стороне должны быть известны параметры кодера, например, вид порождающего полинома, порождающей матрицы, и т.п. Однако возможны ситуации, когда структура кодера неизвестна, например, в результате утери соответствующей информации, ее частичном повреждении, либо при недостаточно оперативном оповещении приемной стороны о смене передающей стороной параметров кодера.

При этом возможны две ситуации. Если используется систематический код, то, хотя возможно выделение информационной последовательности, однако исправление ошибок невозможно, что значительно снижает помехоустойчивость передачи, как правило, значительно ниже допустимых норм. Если же используется несистематический код, то выделение информационной последовательности и исправление

ошибок принципиально невозможно. При этом наступает полный срыв связи.

Однако, обеспечить требуемую помехоустойчивость возможно за счет того, что принимаемые кодовые символы обладают определенными внутренними связями. После соответствующей процедуры диагностики информация о структуре кодера восстанавливается, и помехоустойчивость обеспечивается. Данная статья посвящена возможностям и путям построения диагностических процедур для сверточных кодов.

Теоретическая часть

Рассмотрим некоторые алгоритмы диагностики сверточных кодов и оценим особенности возможной их реализации. Будем считать, что перфорация кодовой последовательности не производится.

Все алгоритмы диагностики построены по единому принципу. Будем рассматривать основную сгенерированную кодовую последовательность \mathbf{u}_0 как совокупность q частных кодовых последовательностей: $\mathbf{u}_1 \div \mathbf{u}_q = \mathbf{g}_1 \mathbf{m} \div \mathbf{g}_q \mathbf{m}$, где $\mathbf{g}_1 \div \mathbf{g}_q$ порождающие полиномы; \mathbf{m} полином исходной информационной последовательности двоичных символов

$$\mathbf{m}(X) = m_0 + m_1 X + m_2 X^2 + m_3 X^3 + \dots + m_i X^i + \dots,$$

где символы m_i принимают значения, равные либо 1, либо 0 в зависимости от передаваемой информации; X – оператор, описывающий задержку по времени на интервал T длительности одного символа (X^2 означает задержку по времени на $2T$, X^3 означает задержку на $3T$, и т.д.).

Используют некоторые «поисковые» полиномы $\mathbf{h}_1 \div \mathbf{h}_q$, вид которых в процессе диагностики изменяется. Преобразования различающихся исходных частных последовательностей символов $\mathbf{u}_1 \div \mathbf{u}_q$ в результате должны формировать одинаковую выходную последовательность \mathbf{m} . Если это достигнуто, то задача диагностики решена. По достижению вышеизложенной цели эти полиномы отождествляются с искомыми порождающими полиномами \mathbf{g}_1 и \mathbf{g}_q .

Рассмотрим кодовую скорость $R=1/2$ (кодер генерирует две частные кодовые последова-

тельности: $\mathbf{u}_1(X) = \mathbf{g}_1(X)\mathbf{m}(X)$ и $\mathbf{u}_2(X) = \mathbf{g}_2(X)\mathbf{m}(X)$), из которых составляется общая кодовая последовательность. Диагностика возможна с помощью различных алгоритмов.

Алгоритм 1. При осуществлении операций этого алгоритма осуществляется двоичное деление частных кодовых последовательностей $\mathbf{u}_1(X)$ и $\mathbf{u}_2(X)$ на некоторые «поисковые» полиномы $\mathbf{h}_1(X)$ и $\mathbf{h}_2(X)$, в результате получаются последовательности:

$$\begin{aligned} \mathbf{y}_1(X) &= \mathbf{u}_1(X)/\mathbf{h}_1(X) = [\mathbf{g}_1(X)/\mathbf{h}_1(X)]\mathbf{m}(X), \\ \mathbf{y}_2(X) &= \mathbf{u}_2(X)/\mathbf{h}_2(X) = [\mathbf{g}_2(X)/\mathbf{h}_2(X)]\mathbf{m}(X). \end{aligned} \quad (1)$$

При осуществлении алгоритма вид полиномов $\mathbf{h}_1(X)$ и $\mathbf{h}_2(X)$ независимо изменяется, и, естественно, при этом меняются и последовательности \mathbf{y}_1 и \mathbf{y}_2 . Когда при этом символы последовательностей $\mathbf{y}_1(X)$ и $\mathbf{y}_2(X)$ станут совпадать, то при условии одинакового значения порядков «поисковых» и искомым полиномов, будет совпадать вид «поисковых» полиномов $\mathbf{h}_1(X)$, $\mathbf{h}_2(X)$ и вид искомым порождающих полиномов $\mathbf{g}_1(X)$, $\mathbf{g}_2(X)$, т.е.: $\mathbf{h}_1(X) = \mathbf{g}_1(X)$ и $\mathbf{h}_2(X) = \mathbf{g}_2(X)$.

Алгоритм 2. При осуществлении операций этого алгоритма обрабатывается одна из частных кодовых последовательностей. (Номер последовательности принципиального значения не имеет, будем рассматривать первую последовательность $\mathbf{u}_1(X)$). Другая последовательность при этом не изменяется.

Первая последовательность подвергается операции $\mathbf{h}_2(X)/\mathbf{h}_1(X)$, т.е., двоичному умножению на полином $\mathbf{h}_2(X)$ и двоичному делению на полином $\mathbf{h}_1(X)$ (порядок осуществления этих операций также значения не имеет). Фактически, умножение на полином является повторным сверточным кодированием последовательности в соответствии с порождающим полиномом $\mathbf{h}_2(X)$.

В результате формируется последовательность символов:

$$\begin{aligned} \mathbf{y}_1(X) &= [\mathbf{h}_2(X)/\mathbf{h}_1(X)]\mathbf{u}_1(X) = \\ &= [\mathbf{h}_2(X)/\mathbf{h}_1(X)]\mathbf{g}_1(X)\mathbf{m}(X). \end{aligned} \quad (2)$$

Она сравнивается с неизменной второй последовательностью $\mathbf{y}_2(X) = \mathbf{g}_2(X)\mathbf{m}(X)$. Случай их совпадения соответствует соблюдению ра-

венства: $[\mathbf{h}_2(X)/\mathbf{h}_1(X)]\mathbf{g}_1(X)=\mathbf{g}_2(X)$, что при заранее известном кодовом ограничении определяет соблюдение равенств: $\mathbf{h}_1(X)=\mathbf{g}_1(X)$; $\mathbf{h}_2(X)=\mathbf{g}_2(X)$.

Алгоритм 3. При осуществлении операций этого алгоритма каждая из частных кодовых последовательностей $\mathbf{u}_1(X)$ и $\mathbf{u}_2(X)$ домножается на «поисковые» полиномы $\mathbf{h}_1(X)$ и $\mathbf{h}_2(X)$, то есть осуществляется повторное сверточное кодирование в соответствии с этими порождающими полиномами.

При этом формируются последовательности символов: $\mathbf{y}_1(X)=\mathbf{h}_1(X)\mathbf{u}_1(X)=\mathbf{h}_1(X)\mathbf{g}_1(X)\mathbf{m}(X)$, и $\mathbf{y}_2(X)=\mathbf{h}_2(X)\mathbf{u}_2(X)=\mathbf{h}_2(X)\mathbf{g}_2(X)\mathbf{m}(X)$. Производится поиск вида полиномов $\mathbf{h}_1(X)$ и $\mathbf{h}_2(X)$ до тех пор, пока символы последовательностей $\mathbf{y}_1(X)$ и $\mathbf{y}_2(X)$ не станут совпадать. Такое возможно, если выполняется условие: $\mathbf{h}_1(X)\mathbf{g}_1(X)=\mathbf{h}_2(X)\mathbf{g}_2(X)$, или $\mathbf{h}_1(X)=\mathbf{g}_2(X)$ и $\mathbf{h}_2(X)=\mathbf{g}_1(X)$. При этом $\mathbf{y}_1(X)=\mathbf{g}_2(X)\mathbf{g}_1(X)\mathbf{m}(X)$, и $\mathbf{y}_2(X)=\mathbf{g}_1(X)\mathbf{g}_2(X)\mathbf{m}(X)$. Поскольку $\mathbf{g}_1(X)\mathbf{g}_2(X)=\mathbf{g}_2(X)\mathbf{g}_1(X)$, то независимо от значения символов последовательности $\mathbf{m}(X)$ будет выполняться равенство $\mathbf{y}_1(X)=\mathbf{y}_2(X)$.

При внешнем сходстве рассмотренные алгоритмы имеют существенные различия в практическом осуществлении, определяющем их достоинства и недостатки. Алгоритмы 1 и 2 включают операцию двоичного деления. Ее стандартная реализация осуществляется несколько сложнее, чем сверточное кодирование (поразрядное умножение по модулю 2). Алгоритм 2 требует двух последовательных операций (умножение и деление), что затрудняет параллелизацию вычислений. В этих условиях алгоритм 3 обладает преимуществами.

Рассмотрим применение вышеописанных алгоритмов. При этом, в соответствии с алгоритмом 1, вид поисковых полиномов будет совпадать с видом искомым порождающих полиномов, если выполняются равенства, аналогичные (1):

$$\mathbf{u}_1/\mathbf{h}_1=\mathbf{u}_2/\mathbf{h}_2=\dots=\mathbf{u}_q/\mathbf{h}_q, \quad (3)$$

т.е. все символы с одинаковыми номерами из новых последовательностей $\mathbf{y}_1 \div \mathbf{y}_q$, которые образованы двоичным делением частных ко-

довых последовательностей $\mathbf{u}_1 \div \mathbf{u}_q$ на соответствующие полиномы $\mathbf{h}_1 \div \mathbf{h}_q$, должны совпадать.

Могут быть предложены различные пути практического осуществления алгоритма. Один из них состоит в том, что все q частных кодовых последовательностей разбиваются на пары, и для всех пар по отдельности определяется вид «поисковых» полиномов в соответствии с алгоритмом для кодовой скорости $R=1/2$.

Другой путь заключается в том, что выбирается одна из частных кодовых последовательностей (скажем, последовательность \mathbf{u}_1), и пары составляются поочередным включением в них этой выбранной кодовой последовательности и остальных $q-1$ частных кодовых последовательностей $\mathbf{u}_2 \div \mathbf{u}_q$.

Представляет интерес более быстрый путь поиска вида порождающих полиномов. Первоначально на основе анализа какой-либо пары частных кодовых последовательностей (скажем, \mathbf{u}_1 и \mathbf{u}_2) определяются «поисковые» полиномы \mathbf{h}_1 и \mathbf{h}_2 . Далее учитывается тот факт, что любое из q равенств $\mathbf{m}(X)=\mathbf{u}_i(X)/\mathbf{g}_i(X)$, $i=1 \div q$ можно переписать в виде: $\mathbf{g}_i(X)=\mathbf{u}_i(X)/\mathbf{m}(X)$. После определения вида порождающих полиномов $\mathbf{g}_1=\mathbf{h}_1$ и $\mathbf{g}_2=\mathbf{h}_2$ «автоматически» оказывается определенным и вид исходной информационной последовательности \mathbf{m} . Поэтому уже эту полученную последовательность можно использовать для непосредственного простого вычисления всех остальных порождающих полиномов, минуя длительную процедуру поиска их вида.

При сравнении свойств изложенных путей реализации алгоритмов можно прийти к следующим выводам. Первый путь представляется более привлекательным, чем второй. Во втором пути при неудачном выборе частной кодовой последовательности, которая включается во все пары или ошибки при нахождении вида \mathbf{g}_1 , могут возникнуть ошибки при определении вида и остальных порождающих полиномов $\mathbf{g}_2 \div \mathbf{g}_q$.

Однако время решения диагностической задачи по второму пути значительно короче.

Действительно, если длина кодового ограничения равна K , то для каждой пары по первому пути возможно $2^K \times 2^K = 2^{2K}$ вариантов сочетаний различных поисковых полиномов. С учетом того, что нужно перебрать $q/2$ пар, общее число исследуемых вариантов полиномов будет составлять $N_1 = (q2^{2K})/2$.

А по второму пути число вариантов сочетаний первой пары равно 2^{2K} . При поиске вида остальных порождающих полиномов исследуется только один полином в паре (т.к. вид другого полинома уже известен). Количество вариантов в этом случае будет равно 2^K . Таким образом, общее число исследуемых вариантов будет равно $N_2 = 2^{2K} + (q-2)2^K$. Нетрудно убедиться, что $N_2 \ll N_1$.

При использовании третьего пути время анализа сокращается в еще большей степени. Вначале на основе двух последовательностей (пусть \mathbf{u}_1 и \mathbf{u}_2) определяется вид двух «поисковых» полиномов \mathbf{h}_1 и \mathbf{h}_2 последовательности \mathbf{m} . Затем производится деление оставшихся последовательностей $\mathbf{u}_3 \div \mathbf{u}_q$ на \mathbf{m} . Поскольку раньше сравнение получаемых последовательностей $\mathbf{y}_1 \div \mathbf{y}_q$ происходило также после деления соответствующих полиномов, то число операций по рассматриваемому третьему пути будет равно: $N_3 = 2^{2K} + (q-2)$, очевидно, что $N_3 \ll N_2$.

Платой за ускорение операции анализа по второму и третьему пути будет увеличение возможности ошибочной диагностики. При неправильном определении хотя бы одной составляющей «поискового» полинома \mathbf{h}_1 по последовательности \mathbf{u}_1 частично неправильными будут и все остальные «поисковые» полиномы,

определенные на его основе. При использовании третьего пути вероятность неправильной диагностики будет еще выше, так как сюда добавляется возможность неправильного восстановления последовательности \mathbf{m} .

Выводы

1. Рассмотрены возможности диагностики сверточных кодов, основанные на определении совпадающих полиномов в частных последовательностях общей кодовой последовательности.
2. Предложены различные алгоритмы обработки кодовых сигналов, основанные на этом принципе.
3. Проанализированы сравнительные возможности предложенных алгоритмов.

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение/ пер. с англ. – М.: Изд. дом «Вильямс», 2003. – 1104с.
2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2006. – 320 с.
3. Полушин П.А., Самойлов А.Г. Избыточность сигналов в радиосвязи. – М.: Радиотехника, 2007. – 256 с.
4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 593 с.
5. Никитин О.Р., Полушин П.А., Белов А.Д., Бессмертный М.Ю. О возможности определения параметров кодера по принимаемому цифровому сигналу / Материалы МНТК «Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2015» (REDS-2015), Москва, 2015. – С. 61-63.

Поступила 11 августа 2015 г.

English

Algorithm development of convolutional codes diagnosis

Natalya Nikolaevna Korneeva - Senior Teacher Radio Engineering&Radio Systems Department Vladimir State University named after Alexander and Nickolay Stoletovs..

E-mail: korneevanata@list.ru.

Oleg Rafailovich Nikitin - Doctor of Engineering, Professor Department Head Radio Engineering and Radio Systems Department Vladimir State University named after Alexander and Nickolay Stoletovs.

E-mail: olnikitin@mail.ru.

Pyotr Alekseevich Polushin – Doctor of Engineering, Professor Radio Engineering and Radio Systems Department Vladimir State University named after Alexader and Nickolay Stoletovs.

E-mail: polushin.p@mail.ru.

Address: 600000, Vladimir, Gorkiy str., 87.

Abstract: Nowadays problems of decoding and error correction remain actual, despite a large number of existing codes. One of the most widespread codes is convolutional coding. It is known that it is necessary to know coder parameters for successful signal recovery in receiving end. In case when these data are missing original signal recovery is not possible. Diagnosis enables to recover coded digital signals even in case of missing or loss of parameters coder information and to decode a signal with error correction that significantly increases information transfer noise stability. Three algorithms for convolutional codes diagnosis are proposed and investigated. Algorithms are examined for different code rates and especially for code rate $R=1/2$.

All algorithms are based on defining matching polynoms in separate sequences of general code sequence. The first algorithm of diagnosis consists in implementation of binary division of private code sequences into search polynoms. When examining the second algorithm processed separate code sequence (any) is exposed to binary division into "its search" polynom and into binary multiplication by polynom of other separate code sequence. The third algorithm implies that each of separate code sequences is multiplied then by "search" polynoms (that is, convolutional coding is repeated according to these generating polynoms). Various ways of practical application of proposed algorithms for convolutional codes diagnosis are examined.

One of the ways involves splitting all separate code sequences into pairs and defining pairs type of "search" polynoms. The other way implies that one of separate code sequences is selected and pairs are formed through successive engagement of this selected code sequence in them. Any separate code sequences pair is analyzed and their "search" polynoms are defined when we consider the third way. Type of partial original information sequence is defined "automatically" after generating polynoms type is defined. Therefore already obtained sequence can be used for direct calculation of all other generating polynoms without long procedure for searching their type.

Key words: convolutional coding, noiseproof information transmission, "search" polynoms, generating polynoms.

References

1. Sklar B. Digital Communications: Fundamentals and Applications. - transl. from English - M.: Publ. house "Williams", 2003. – 1104p.
2. Morelos-Zaragoza R. The Art of Error Correcting Coding. Methods, algorithms, application. - M.: Tekhnosfere, 2006. - 320 p.
3. Polushin P. A., Samoylov A.G. Signals redundancy in radio communication. - M.: Radiotekhnika, 2007. - 256 p.
4. Peterson W., Weldon E. Error-correcting codes. - M.: Mir, 1976. - 593 p.
5. Nikitin O. R., Polushin P. A., Belov A.D., Beesmrtny M. Yu. On possibility to define coder parameters by received digital signal. - Materials ISTC "Radio-electronic devices and systems for information communication technologies - REUS-2015" (REDS-2015), Moscow, 2015. – P. 61-63.