себя непредсказуемым образом. А об этом люди смогут узнают, только когда станет слишком поздно. Пока, никто не знает, будут ли изменения ИИ и их попытки внедрения в жизнь людей положительными для самих людей или нас ждет неопределенный конец, хотя некоторые возлагают большие надежды.

В заключении отметим, развитие ИИ со временем приобретает все большую популярность, ведь он имеет некоторую прерогативу, однако выдающимся умам еще не довелось создать полностью совершенного интеллекта. Ответ на вопрос, какое будущее принесет нам ИИ и нейронные сети, остается открытым, по сей день.

Список использованных источников:

1. Тьюринг, А. М. Вычислительные машины и разум/А. М. Тьюринг //Глаз разума /Д. Хофштадтер, Д. Деннетт. – Самара: Бахрах-М, 2003. – С. 47–59.
2. Компьютер учится и рассуждает (ч. 1) // Компьютер обретает разум = Artificial Intelligence Computer Images / под ред. В. Л. Стефанюка. – Москва: Мир, 1990. – 240 с.
3. Девятков, В.В. Системы искусственного интеллекта / В.В. Девятков. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2001. – 352 с.
4. AIportal [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.aiportal.ru/articles/neural-networks/neural-networks.html. Дата доступа 15.03.2018.

ДЕКОДИРОВАНИЕ ОРТОГОНАЛЬНОГО НЕЛИНЕЙНОГО КОДА

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Хадкевич О.В.

Митюхин А. И. – доцент каф. ФМД

В работе рассматривается задача декодирования нелинейного помехоустойчивого ортогонального кода, обеспечивающего коррекцию ошибок и защиту информации в основном информационном канале и в канале с подслушиванием.

Одно из применений нелинейных ортогональных помехоустойчивых $[N, M, d]$-кодов длиной N и кодовым расстоянием d заключается в коррекции ошибок – обнаружении и исправлении t ошибок в канале с аддитивным гауссовским шумом $n(i)$ [1]. Другое применение – это обеспечение определенного уровня защиты информации от несанкционированного доступа. Свойство нелинейности кода позволяет иметь значительно больший ансамбль M кодовых слов над полем Галуа $\{F\}$ в сравнении с линейными кодами, что важно для защиты информации. Рассматривается подход решения задачи декодирования помехоустойчивого кода для системы, в которой предусмотрена защита информации и коррекция ошибок. Предполагается, что преднамеренные генерируемые ошибки в принятом сигнале в канале подслушивания должны мешать правильному декодированию перехватываемой информации.

Пусть слова кода $\boldsymbol{X} = \boldsymbol{X}^1, \boldsymbol{X}^2, \dots, \boldsymbol{X}^s, \dots, \boldsymbol{X}^M$, $\boldsymbol{X}^s = (x(1), \dots, x(N))$ передаются по основному каналу с шумом $n(i)$. Структура кодовых слов $\{\boldsymbol{X}\}$ априори известна на приемной стороне. На выходе канала формируется аддитивный процесс

$$y^s(i) = x^s(i) + n^s(i), i = 1, 2, \dots, N, \quad (1)$$

который можно представить в виде вектора наблюдения $\boldsymbol{Y^s} = (y(1), \dots, y(N))$. Экспериментально вычисляя вероятности $P(\boldsymbol{Y^s})$ на множестве $\{\boldsymbol{Y}\}$, имея априорные значения вероятностей $\{P(\boldsymbol{X})\}$ кодовых слов (входа канала) и зная свойства канала – переходные вероятности $P(\boldsymbol{Y}|\boldsymbol{X^s})$, можно найти вероятность $P(\boldsymbol{X^s}|\boldsymbol{Y})$ – вероятность получения слова $\boldsymbol{X^s}$ кода $\boldsymbol{X}$ на приемной стороне (выходе канала). В соответствии с теоремой Байеса вероятность получения слова входа основного канала, при условии, что на выходе канала уже получен вектор $\boldsymbol{Y}$, определяется как

$$P(\boldsymbol{X^s}|\boldsymbol{Y}) = \frac{P(\boldsymbol{Y}|\boldsymbol{X}^s)P(\boldsymbol{X}^s)}{\boldsymbol{P}(Y^s)}. \quad (2)$$

Так как вероятности $P(\boldsymbol{X}^s)$ и $P(\boldsymbol{Y^s})$ известны, отношение $\frac{P(\boldsymbol{X}^s)}{\boldsymbol{P}(Y^s)}$ равно постоянной величине $K = \frac{P(\boldsymbol{X}^s)}{\boldsymbol{P}(Y^s)}$. Выражение (2) примет вид $P(\boldsymbol{X^s}|\boldsymbol{Y}) = K\, P(\boldsymbol{Y}|\boldsymbol{X}^s)$. Из последней записи следует, что процедура декодирования по основному каналу заключается в нахождении такого значения номера s кодового слова, при котором значение апостериорной вероятности $P(\boldsymbol{X^s}|\boldsymbol{Y})$ достигает максимума. Таким образом, декодирование требует вычисления max $P(\boldsymbol{Y}|\boldsymbol{X}^s)$ – вероятности получения $\boldsymbol{Y}$ при условии, что было передано кодовое слово $\boldsymbol{X}^s$. Если $\boldsymbol{Y} = \boldsymbol{X}^s$, достигается max $P(\boldsymbol{Y}|\boldsymbol{X}^s)$ и обеспечивается прием с нулевой вероятностью ошибок. Поскольку из (1) $y^s(i) - x^s(i) = n^s(i)$, функцию $P(\boldsymbol{Y}|\boldsymbol{X}^s)$ отобразим как

$$P(\boldsymbol{Y}|\boldsymbol{X}^s) = P(\boldsymbol{Y} - \boldsymbol{X}^s = \boldsymbol{n}) = P(\boldsymbol{n}),$$

где $\{\boldsymbol{n}\}$ – множество преднамеренных шумовых векторов, $P(\boldsymbol{n})$ – вероятности векторов шума. Выражение $\{\boldsymbol{Y} - \boldsymbol{X}^s\}$ – это множество $\{d_x\}$ расстояний Хемминга между словом $\boldsymbol{Y}$ на входе декодера и всеми словами кода. С позиции теории кодирования d_x показывает, сколько символов в слове надо исказить, чтобы перевести одно разрешенное для передачи кодовое слово в другое разрешенное. Тогда вычисление функции max $P(\boldsymbol{Y}|\boldsymbol{X}^s)$ сводится к нахождению опорного кодового вектора $\boldsymbol{X}^s$ ближайшего по расстоянию Хемминга к принятому вектору $\boldsymbol{Y}$ (на выходе канала). Если использовать пространственную интерпретацию кода как множество точек (векторов) *N*-мерной решетки, то вероятность того, что точка $\boldsymbol{X}^s$ совпадет с точкой $\boldsymbol{Y}$, увеличивается с уменьшением евклидова расстояния. Степень близости точек $\boldsymbol{X}^s$ и $\boldsymbol{Y}$ в пространстве размерностью N легко вычисляется с помощью скалярного произведения

$$\langle \boldsymbol{Y}|\boldsymbol{X}^s\rangle = \sum_{i=1}^{N} y(i)\, x^s(i) \qquad (3)$$

векторов, описывающих точки. Эта операция лежит в основе декодирования по основному каналу. Из проведенного анализа следует, что для успешного перехвата информации по каналу подслушивания необходимо иметь априорные знания об основных параметрах кода, в частности, мощности множества $\{\boldsymbol{X}\}$ и переходных вероятностях канала. Задача декодирования еще более усложняется, когда шум используется с целью маскирования информации. Тогда декодирование должно выполняться по вектору наблюдения $\boldsymbol{Y} = \boldsymbol{X} + \boldsymbol{n}$. Отсутствие точной информации об алгебраической структуре кода $\boldsymbol{X}$ и множестве случайных векторов $\{\boldsymbol{n}\}$ в канале с подслушиванием не позволяет перехватчику декодировать сигнал $\boldsymbol{Y}$ по алгоритму (3). Решение задачи перехвата на основе многоканальной обработки по (3) и перебором последовательностей $\boldsymbol{X}$ и $\boldsymbol{n}$ потребует значительных вычислительных, временных и технических ресурсов.

Список использованных источников.

1. Митюхин, А.И. Корреляционные спектры и кодовые расстояния мажоритарных последовательностей/А.И. Митюхин, П.Н. Якубенко// Доклады БГУИР. – 2015. № 4 (90). − С. 5–9.

ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ НИЗКОСКОРОСТНОГО КОДИРОВАНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шлома К.Н.

Митюхин А. И. – доцент каф. ФМД

Анализируется один из основных сервисов информационной безопасности – помехоустойчивое кодирование и защита информации от несанкционированного доступа в радиоэлектронных системах. Рассматривается система кодирования информации с использованием множества неприводимых полиномов над полем $GF(2)$ в каналах с гауссовским шумом. Дана оценка возможных временных затрат декодирования при приеме кодированных данных в условиях априорной неопределенности.

Для обеспечения информационной безопасности при передаче данных используются помехоустойчивые коды. Защита информации в специальных радиоэлектронных системах гражданского и военного назначения от воздействия непреднамеренных и преднамеренных помех осуществляется посредством низкоскоростного помехоустойчивого кодирования [1]. Кроме защиты информации от ошибок (коррекции информации) в каналах с шумами, такие коды над конечным полем $GF(q)$ обеспечивают определенную степень безопасности информационных комплексов от случайного и несанкционированного доступа к информации. Решение этой задачи основывается на применении множества изменяющихся во времени $[n, k, d]$-кодов

$$\boldsymbol{C} = \{\boldsymbol{C^1}, \dots, \boldsymbol{C^J}, \dots, \boldsymbol{C^L}\}, \boldsymbol{c^j} \in \boldsymbol{C^J}, c^j = (c_1, \dots, c_i \dots, c_n), c_i \in GF(q),$$

где k – размерность *j*-кода, $n = q^k - 1$ – длина *j*-кода, d – минимальное расстояние *j*-кода (характеризует корректирующую способность кода), $\boldsymbol{c}^j$– кодовая последовательность с символами из поля $GF(q)$, $M = q^k$–1 – количество слов *j*-кода (мощность множества), q – простое число (основание кода). Практическая алгебраическая конструкция псевдошумового низкоскоростного $[n, k, d]$-кода основывается на применении неприводимого над полем $GF(2)$ полинома вида

$$h(x) = 1 + h_1 x + \cdots + h_{m-1} x^{m-1} + h_m x^m,$$

где коэффициенты $h_i \in \{0, 1\}$, $k = m$. Число возможных различных неприводимых над полем $GF(2)$ полиномов $h(x)$ степени m определяется по формуле