

ПОСТРОЕНИЕ СВЕРТОЧНЫХ КОДОВ

к.т.н. С.И. Приходько
(представил д.т.н. проф. В.И. Долгов)

Рассмотрены конструктивные процедуры построения сверточных кодов с заданными характеристиками, базирующиеся на алгебраическом представлении.

Для защиты информации от ошибок в настоящее время все более широкое применение находят сверточные коды. Существенным недостатком, снижающим эффективность их применения, является отсутствие алгебраических процедур, определяющих их построение [1].

Для решения этой задачи зададим \mathbf{m} многочленов сверточного $(\mathbf{n}_0, \mathbf{R}_0)$ кода под полем $\mathbf{GF}(p)$ с помощью одного многочлена $\mathbf{F}(x)$ под полем $\mathbf{GF}(p^m)$. Это обобщенное представление сверточных кодов. Такой обобщенно заданный сверточный код будет иметь скорость $\mathbf{R} = \frac{1}{m}$ и длину

кодировочного ограничения $\mathbf{n}_{\text{ск}} = (\mathbf{u} + 1)\mathbf{n}_0$, где \mathbf{u} - степень многочлена $\mathbf{F}(x)$. В этом случае работа сверточного кодирующего устройства может быть определена следующим образом. На вход кодера поступает информационная последовательность, заданная многочленом $\mathbf{M}(x)$ под полем $\mathbf{GF}(p)$. В кодере происходит умножение многочлена $\mathbf{M}(x)$ на $\mathbf{F}(x)$ и получение многочлена $\mathbf{T}(x)$ над полем $\mathbf{GF}(p^m)$. Далее многочлен $\mathbf{T}(x)$ отображается в поле $\mathbf{GF}(p)$. Полученный таким образом многочлен $\mathbf{T}(x)$ над полем $\mathbf{GF}(p)$ будет являться кодовым словом сверточного $(\mathbf{n}_0, \mathbf{k}_0)$ кода со скоростью $\mathbf{R} = \frac{1}{m}$ над полем $\mathbf{GF}(p)$ и длиной кодировочного ограничения $\mathbf{n}_{\text{ск}} = (\mathbf{u} + 1)\mathbf{m}$.

Обобщенное представление сверточных кодов позволяет использовать зависимость между корнями многочлена $\mathbf{F}(x)$ и кодовым расстоянием соответствующего сверточного кода. Возможны две ситуации. В пер-

вом случае кода $n_{\text{ск}} < n$, где n - длина кодового слова циклического кода над полем $\text{GF}(p^m)$ с кодовым расстоянием d , задаваемого многочленом $F(x)$, минимальное кодовое расстояние d_m обобщенно заданного сверточного кода будет определяться из соотношения $d_m \geq d$. Во втором случае, когда $n_{\text{ск}} > n$, необходимо учитывать возможное уменьшение кодового расстояния, когда $M(x) \cdot F(x) = (x^n - 1) \cdot R(x)$ и многочлен $R(x)$ имеет малый вес. Тогда в первом случае построение сверточного кода над полем $\text{GF}(p)$ со скоростью $R = \frac{1}{m}$ сводится к выбору соответ-

ствующего многочлена $F(x)$ над полем $\text{GF}(p^m)$, причем, если $n_{\text{ск}} < n$, то кодовое расстояние сверточного кода гарантируется кодовым расстоянием соответствующего циклического кода. Если $n_{\text{ск}} > n$, то при построении сверточного кода необходимо учитывать выбор многочлена $R(x)$. Его вес должен быть большим и может быть определен с помощью последовательности его корней. Следует заметить, что в первом и втором случаях необходимо учитывать вариант отображения $\text{GF}(p^m)$ в поле $\text{GF}(p)$.

Для построения сверточных кодов со скоростью $R = k_0/n_0$ необходимо использовать суперпозицию обобщенно заданных порождающих многочленов $F(x)$ сверточных кодов. В этом случае, процедуру кодирования сверточным кодом можно представить следующим образом. На вход поступает k_0 информационных последовательностей, задаваемых многочленами $M_i(x)$, где $i = \overline{1, k_0}$ с коэффициентами из поля $\text{GF}(p)$. Далее происходит получение k_0 произведений $T_i(x) = M_i(x) \cdot F_i(x)$, причем, в общем случае, коэффициенты у многочленов T_i принадлежат полю $\text{GF}(p^m)$. Следующим этапом является операция суперпозиции многочленов T_i для получения многочлена $T(x)$, являющегося кодовым словом сверточного кода в обобщенной форме. В качестве процедуры суперпозиции можно использовать прямое произведение кодов, где кодовыми словами исходных кодов являются многочлены $T_i(x)$. Затем многочлен $T(x)$ над полем $\text{GF}(p^m)$ отображается в многочлен над полем $\text{GF}(p)$, который и является кодовым словом сверточного (n_0, k_0) кода над полем $\text{GF}(p)$ со скоростью $R = k_0/n_0$.

Положительным свойством такой процедуры является возможность рассмотрения обобщенного кодирования сверточных кодов со скоростью $R = k_0/n_0$ как каскадного кодирования. Тогда процедура состоит из трех

ступеней. Первые две ступени включают в себя процедуру $M_i(x) \cdot F_i(x)$ и процедуру $T_1(x) \cdot T_2(x) \cdot \dots \cdot T_R(x)$, а кодовое расстояние будет определяться минимальным весом $T_i(x)$. Таким образом, в результате первого этапа каскадного кодирования, кодовое расстояние обобщенного сверточного кода будет определяться как $d_m \geq \{d, 2d'\}$, где d' - минимальный вес многочлена $R(x)$. Обозначим через (n_i, R_i, d_i) - параметры кодов, задаваемых многочленами $F_i(x)$ над полем $GF(p^m)$. Тогда, в результате прямого кодирования кодов, код, полученный на втором этапе каскадного кодирования, имеет параметры $(n_1 \cdot n_2 \cdot \dots \cdot n_R, R_1 \cdot R_2 \cdot \dots \cdot R_R, d_1 \cdot d_2 \cdot \dots \cdot d_R)$.

Если особым образом не осуществить выбор многочленов $F_1(x)$ и $F_2(x)$ над полем $GF(p^m)$, то результат прямого произведения не будет циклическим кодом, хотя будет всегда линейен [2]. На этапе 3 кодирования происходит отображение многочлена $T(x)$ над полем $GF(p^m)$ в многочлен над полем $GF(p)$. Каждый элемент $GF(p^m)$ представляется символами $GF(p)$.

При выборе любого базиса многочлен $T(x)$ над полем $GF(p)$ будет являться кодовым словом линейного кода. Осуществляя отображение, можно, за счет дополнительных преобразований увеличить кодовое расстояние, например, вводя общую проверку на четность каждого коэффициента многочлена $T(x)$. Если обобщенный сверточный код имеет параметры (n_0, k_0) и кодовое расстояние d_m , то в результате третьего этапа код будет иметь параметры $(m \cdot n_0, m \cdot k_0)$. После добавления общей проверки на четность полученный код над полем $GF(p)$ будет иметь параметры:

$$n = (m + 1)(p^m - 1); R = mR_0; d \geq d + 1.$$

Полученные результаты позволили синтезировать алгоритмы построения сверточных кодов с заданными характеристиками с учетом рассмотренных особенностей. Построенные сверточные коды сравнивались для различных скоростей с известными [1] сверточными кодами. Сравнение показало, что полученные результаты не уступают известным, а при применении процедуры каскадирования их превосходят, что подтверждает целесообразность использования рассмотренных конструкций.

ЛИТЕРАТУРА

1. Теория кодирования /Кисами Т., Топура Н. и др. - М.: Мир, 1978. - 342 с.

2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. - М.: 1986. - 144 с.