УДК 621.391

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 $\mathbf{(n_0, R_0)}$ 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 кодового ограничения $\mathbf{n_{ск} = (u + 1)n_0}$, 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 $\mathbf{(n_0, k_0)}$ кода со скоростью $\mathbf{R = \frac{1}{m}}$ над полем $\mathbf{GF(p)}$ и длиной кодового ограничения $\mathbf{n_{ск} = (u + 1)m}$.

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 $n_{ск} < n$, где n - длина кодового слова циклического кода над полем $GF(p^m)$ 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 $n_{ск} > n$, 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 $GF(p)$ со скоростью $R = \frac{1}{m}$ сводится к выбору соответствующего многочлена $F(x)$ над полем $GF(p^m)$, причем, если $n_{ск} < n$, то кодовое расстояние сверточного кода гарантируется кодовым расстоянием соответствующего циклического кода. Если $n_{ск} > n$, 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 $GF(p^m)$ в поле $GF(p)$.

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 $GF(p)$. 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 $GF(p^m)$. 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 $GF(p^m)$ отображается в многочлен над полем $GF(p)$, который и является кодовым словом сверточного (n_0, k_0) кода над полем $GF(p)$ 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 $\mathbf{M_i(x) \cdot F_i(x)}$ и процедуру $\mathbf{T_1(x) \cdot T_2(x) \cdot ... \cdot T_R(x)}$, а кодовое расстояние будет определяться минимальным весом $\mathbf{T_i(x)}$. Таким образом, в результате первого этапа каскадного кодирования, кодовое расстояние обобщенного сверточного кода будет определяться как $\mathbf{d_m \geq \{d, 2d'\}}$, где $\mathbf{d'}$ - минимальный вес многочлена $\mathbf{R(x)}$. Обозначим через $\mathbf{(n_i, R_i, d_i)}$ - параметры кодов, задаваемых многочленами $\mathbf{F_i(x)}$ над полем $\mathbf{GF(p^m)}$. Тогда, в результате прямого кодирования кодов, код, полученный на втором этапе каскадного кодирования, имеет параметры $\mathbf{(n_1 \cdot n_2 \cdot ... \cdot n_R, R_1 \cdot R_2 \cdot ... \cdot R_R, d_1 \cdot d_2 \cdot ... \cdot d_R)}$.

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

При выборе любого базиса многочлен $\mathbf{T(x)}$ над полем $\mathbf{GF(p)}$ 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 $\mathbf{T(x)}$. Если обобщенный сверточный код имеет параметры $(\mathbf{n_0, k_0})$ и кодовое расстояние $\mathbf{d_m}$, то в результате третьего этапа код будет иметь параметры $\mathbf{(m \cdot n_0, m \cdot R_0)}$. После добавления общей проверки на четность полученный код над полем $\mathbf{GF(p)}$ будет иметь параметры:

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

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.