ГРАНИЦА ПЛОТКИНА ДЛЯ СВЕРТОЧНЫХ КОДОВ

В. И. Долгов

Харьков

Интерес, проявленный к последовательному, а затем и к пороговому декодированию, привел к быстрому развитию теории сверточных кодов [1, 2, 3, 4].

Однако проблема систематического построения сверточного кода, способного исправлять большое число ошибок при заданной длине кодового ограничения, окончательно не решена.

В настоящей статье обсуждается граница Плоткина применительно к сверточным кодам, имеющим скорость $R = \frac{1}{n_0}\log_2 q$, при этом предполагается, что все операции выполняются в поле $GF(q)$.

Рассмотрим множество начальных кодовых слов сверточного кода, в которых хотя бы один из множества первых информационных символов отличен от нуля. Такое множество определяет средний вес кодового слова в этом сверточном коде [2]. Его можно получить из множества всех начальных кодовых слов, имеющих все первые информационные символы равные нулю, сложив по модулю q каждое из них с некоторым начальным кодовым словом, в котором хотя бы один из множества первых информационных символов отличен от нуля.

Множество всех начальных кодовых слов, в которых все первые информационные символы равны нулю, образует подгруппу, и, следовательно, для него выполняется граница Плоткина [3] для линейных (n, k)-кодов. Для сверточного кода с длиной кодового ограничения n_A и скоростью $R = \frac{1}{n_0}\log_2 q$ имеем

$$d_0 \leqslant \frac{(n_A - n_0)\, q^{R(n_A - n_0)-1}(q-1)}{q^{R(n_A - n_0)} - 1}. \qquad (1)$$

Длина кода n соответствует здесь величине $n_A - n_0$, а количество информационных символов k — величине $R(n_A - n_0)$; d_0 — минимальный вес кода, в котором все первые информационные символы равны нулю. Если же учесть, что при сложении по модулю q каждого из множества начальных кодовых слов, в которых все первые информационные символы равны нулю, с некоторым начальным кодовым словом, в котором хотя бы один из множества первых информационных символов отличен от нуля, минимальный вес кода может измениться максимум на n_0 единиц, то тогда имеем

$$d \leqslant d_0 + n_0, \qquad (2)$$

где d — минимальное расстояние сверточного кода [2].

Подставляя (1) в (2), получим

$$d < \frac{(n_A - n_0)\, q^{R(n_A - n_0)-1}(q-1)}{q^{R(n_A-n_0)}-1} + n_0. \qquad (3)$$

Этот результат можно записать в виде теоремы. Минимальный вес d сверточного кода с длиной кодового ограничения n_A и скоростью $R = \frac{1}{n_0}\log_2 q$ удовлетворяет неравенству

$$d < \frac{(n_A - n_0)\, q^{R(n_A-n_0)-1}(q-1)}{q^{R(n_A-n_0)}-1} + n_0.$$

Если сравнить этот результат с аналогичным, имеющимся в [2], то легко убедиться, что разница в оценке d составляет величину $\frac{(n_A - n_0)}{q^{R(n_A-n_0)}-1} \times$ $\times \frac{(q-1)}{q} \ll 1$; а если учесть, что для определения d нужно брать только целую часть числа, то получается, что оценки практически совпадают.

Кроме того, можно сделать и следующий вывод. Среди всех сверточных кодов с длиной кодового ограничения n_A и скоростью $R = \frac{1}{n_0}\log_2 q$ только тот может достичь границы Плоткина (3), в котором все первые n_0 символов отличны от нуля.

В дальнейшем нам понадобится следующая теорема, доказательство которой приведено в [3]. Если $n > d$, то

$$B(n, d) \leqslant qB(n-1, d), \qquad (4)$$

где $B(n, d)$ — максимально возможное число кодовых слов линейного кода длины n с минимальным весом, не меньшим d.

Переписываем формулу (1)

$$d_0\left(q^{R(n_A-n_0)}-1\right) < (n_A - n_0)\, q^{R(n_A-n_0)}\,\frac{q-1}{q}, \qquad (5)$$

или

$$q^{R(n_A-n_0)}\left[qd_0 - (n_A - n_0)(q-1)\right] < qd_0. \qquad (6)$$

Если

$$qd_0 - (n_A - n_0)(q-1) > 0, \qquad (7)$$

то

$$q^{R(n_A-n_0)} = B(n_A - n_0,\ d_0) < \frac{qd_0}{qd_0 - (n_A - n_0)(q-1)}, \qquad (8)$$

где $B(n_A - n_0, d_0)$ — максимально возможное число кодовых слов линейного кода, составленного из начальных кодовых слов сверточного кода, в которых все первые информационные символы равны нулю с минимальным весом, не меньшим d_0.

Для случая

$$n_A - n_0 = \frac{qd_0 - 1}{q-1} \qquad (9)$$

$$B\left(\frac{qd_0-1}{q-1},\ d_0\right) < qd_0. \qquad (10)$$

Применяя многократно теорему [3], получаем

$$B(n_A - n_0,\ d_0) \leqslant q^a B(n_A - n_0 - a,\ d_0). \qquad (11)$$

Комбинируя неравенства (10) и (11) при $n_A - n_0 - a = \frac{qd_0 - 1}{q-1}$, получим

$$B(n_A - n_0, d_0) \leqslant q^a B\left(\frac{qd_0 - 1}{q-1}, d_0\right) \leqslant q^{n_A - n_0 - \frac{qd_0 - 1}{q-1}} qd_0. \quad (12)$$

Поскольку для кода с максимальным минимальным расстоянием

$$B(n_A - n_0, d_0) = q^{R(n_A - n_0)}, \quad (13)$$

где $R(n_A - n_0)$ число информационных символов этого кода, то

$$R(n_A - n_0) \leqslant n_A - n_0 - \frac{qd_0 - 1}{q-1} + \log_q d_0 + 1; \quad (14)$$

или, разрешая относительно R, получим

$$R \leqslant 1 - \frac{1}{n_A - n_0}\left(\frac{qd_0 - 1}{q-1} - \log_q d_0 - 1\right). \quad (15)$$

Если же учесть, что всегда $d_0 \leqslant d$ и (2), то (15) можно записать в виде

$$R \leqslant 1 - \frac{1}{n_A - n_0}\left(\frac{qd}{q-1} - \frac{1}{q-1} - \log_q (d - n_0) - 1\right). \quad (16)$$

Эта запись означает, что если выполняется (16), то выполняется и (15).

Таким образом, верна следующая теорема.

Теорема. Если $n_A - n_0 \geqslant \frac{qd-1}{d-1}$, то для того, чтобы минимальный вес сверточного кода с длиной кодового ограничения n_A достигал значения d, необходимо, чтобы этот код имел скорость $R = \frac{1}{n_0}\log_2 q$, равную самое большее

$$1 - \frac{1}{n_A - n_0}\left(\frac{qd}{q-1} - \frac{1}{q-1} - \log_q (d - n_0) - 1\right).$$

ЛИТЕРАТУРА

1. Дж. Возенкрафт, Б. Райффен. Последовательное декодирование. Изд-во иностр. лит-ры, 1963.
2. Дж. Мэсси. Пороговое декодирование. Изд-во иностр. лит-ры, 1966.
3. У. Питерсон. Коды, исправляющие ошибки. Изд-во иностр. лит-ры, 1964.
4. Ж. Джулиан, Бусганг. Некоторые свойства порождающих последовательностей двоичных сверточных кодов. IEEE Transactions on Information Theory., January, 1965. v. IT — 11. N 1.