§ 10. Модификация кодов

Любой код имеет три фундаментальных параметра — длину n, размерность k и избыточность $r = n-k$. Фиксируя один из этих параметров и изменяя (увеличивая либо уменьшая) другой, мы получаем 6 возможных приемов модификации кодов:

1) *аугментация* — n фиксировано, k увеличивается, r уменьшается;

2) *элиминация* — n фиксировано, k уменьшается, r увеличивается;

3) *расширение* — k фиксировано, n увеличивается, r увеличивается;

4) *сужение* — k фиксировано, n уменьшается, r уменьшается;

5) *удлинение* — r фиксировано, n увеличивается, k увеличивается;

6) *укорочение* — r фиксировано, n уменьшается, k уменьшается.

Аугментация и элиминация. При аугментации кода к нему добавляются новые кодовые слова. Обратный процесс элиминации состоит в отбрасывании ряда кодовых слов.

Заметим, что при аугментации минимальное расстояние может уменьшиться, в то время как при элиминации, напротив, возрасти. Для обобщенных кодов Рида-Соломона справедливо

$$GRS_{n,k-1}(\alpha, v) \subset GRS_{n,k}(\alpha, v).$$

Второй код здесь получается аугментацией первого, а первый — элиминацией второго. В данном случае элиминированный код имеет строго большее минимальное расстояние.

Для линейного кода процесс аугментации может быть произведен путем добавления нескольких строк к порождающей матрице, а процесс элиминации — путем вычеркивания нескольких строк. Типичный способ аугментации линейного кода состоит в добавлении к порождающей матрице строки из одних единиц.

Поскольку увеличение размера линейного кода равносильно уменьшению размера дуального к нему кода, эти два способа модификации кодов не только взаимно обратны друг к другу, но и взаимно дуальны. Дуальный к аугментированному посредством приписывания строки единиц коду получается из исходного дуального

кода элиминацией, при которой оставляются только те кодовые слова, сумма координат которых равна 0.

Аугментация и элиминация могут применяться также и к нелинейным кодам. Пусть C — линейный код, являющийся подкодом линейного кода D. Можно построить новый код, не обязательно линейный, являющийся аугментацией C и элиминацией D, путем добавления к C некоторых его смежных классов в D. Например, можно выбрать те смежные классы, лидеры которых имеют наибольший вес. Подобный прием конструирует некоторые нелинейные коды, которые имеют лучшие свойства (в данном случае минимальное расстояние), чем любые линейные коды той же длины и того же размера.

Расширение и сужение. При расширении кода к нему добавляются дополнительные избыточные символы. Обратный процесс — сужение удаляет избыточные символы. Эти приемы модификации обладают тем свойством, что получаемый код взаимно однозначно соответствует исходному коду. Сужение может уменьшить минимальное расстояние, расширение — увеличить. Для расширения линейного кода добавляются новые столбцы к порождающей матрице кода, в процессе сужения некоторые столбцы вычеркиваются.

Будем называть линейный $[n+1, k]$-код C^+ *координатным расширением* кода C, если он получается добавлением одного нового избыточного символа к линейному $[n, k]$-коду C над полем F. Каждое кодовое слово $c^+ = (c_1, \ldots, c_n, c_{n+1})$ расширенного кода C^+ получается добавлением к кодовому слову $c = (c_1, \ldots, c_n)$ кода C новой координаты $c_{n+1} = \sum_{i=1}^{n} a_i c_i = a \cdot c$ для некоторого фиксированного $a = (a_1, \ldots, a_n) \in F^n$. Здесь в качестве новой координаты мы берем последнюю, хотя это новый символ может быть помещен в любую координатную позицию исходного кода.

Будем предполагать, что $a \notin C^\perp$. (В противном случае, если бы a принадлежало $C^\perp$, всегда было бы $c_{n+1} = 0$.) Будем называть подкод $C_0 = C \cap a^\perp$ кода C, имеющий размерность $k-1$, *ядром* расширения. При замене вектора a любым другим вектором смежного класса $a + C^\perp$ не меняет расширение C^+ и ядро C_0.

Если G_0 — порождающая матрица ядра C_0 и $c \in C - C_0$, то порождающая матрица для координатного расширения C^+ имеет вид

$$\left(\begin{array}{c|c} G_0 & 0 \\ \hline c & c_{n+1} \end{array}\right)$$

Наиболее типичным способом расширения кода является присоединение символа проверки на четность, последнего символа, выбираемого с таким расчетом, чтобы сумма всех координат новых кодовых слов всегда была равно 0. Это соответствует координатному расширению с вектором $a = (-1, -1, \ldots, -1)$. В случае, когда C — двоичный код Хэмминга, такое расширение приводит к расширенному коду Хэмминга с минимальным расстоянием 4. Независимо от того, какую координатную позицию теперь мы выберем для сужения расширенного кода Хэмминга, в результате получим код с минимальным расстоянием 3, являющийся обычным кодом Хэмминга.

Удлинение и укорочение. При удлинении кода увеличивается его длина и добавляются новые кодовые слова. Обратный процесс — укорочение заключается в отбрасывании некоторых кодовых слов и вычеркивании некоторых координатных позиций. Таким образом, данные операции могут рассматриваться как комбинации рассмотренных выше. Удлинение есть расширение с последующей аугментацией, укорочение есть элиминация с последующем сужением. Так как комбинируемые операции влияют на минимальное расстояние противоположным образом, действительное воздействие удлинения или укорочения на минимальное расстояние зависит от ситуации.

Для линейных кодов удлинение соответствует окаймлению порождающей матрицы путем добавления новых столбцов (расширение) и такого же числа новых строк (аугментация). Стандартный способ удлинения состоит в том, чтобы добавить нулевой столбец, а затем добавить строку, содержащую ненулевой элемент в этом новом столбце (например, вектор из единиц). Таким образом, координатное расширение D^+ линейного кода D представляет собой удлинение его ядра $C = D_0$. Удлинение кода — действие, дуальное расширению, и специальный случай добавления столбца из 0 с последующим добавлением строки из 1 соответствует расширению $C^\perp$ дополнительным символом проверки на четность. Именно так в §7, исходя из лексикографической порождающей матрицы L_m для дуального кода Хэмминга C, окаймляя ее, мы построили порождающую матрицу EL_m для кода Рида-Маллера первого порядка $RM(1, m)$, дуального к расширенному коду Хэмминга.

Задача. Пусть C^+ — координатное расширение линейного кода C с ядром C_0. Докажите, что $(C^+)^\perp$ есть расширение $C_0^\perp$ и удлинение $C^\perp$.