МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
А. В. Чашкин

ЛЕКЦИИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ

Учебное пособие

Москва · 2007

Содержание

1 Линейные коды

Код G называется линейным $(n,\ k)$-кодом, если он является k-мерным линейным подпространством пространства $\mathbb{B}^n$. Справедлива следующая теорема о кодовом расстоянии линейного кода.

Теорема 1.1 *В каждом линейном коде G кодовое расстояние d равно весу его минимальноого ненулевого элемента:*

$$d = \min_{\mathbf{g}\neq 0, \mathbf{g}\in G} ||\mathbf{g}||.$$

ДОКАЗАТЕЛЬСТВО. Так как нулевой набор всегда принадлежит линейному коду, то, очевидно, что кодовое расстояние не превосходит веса минимального ненулевого элемента. Допустим, что $d < min||\mathbf{g}||$. В этом случае в G найдутся два элемента $\mathbf{g_1}$ и $\mathbf{g_2}$, расстояние между которыми меньше d. Следовательно,

$$||\mathbf{g}_1 \oplus \mathbf{g}_2|| = d(\mathbf{g}_1, \mathbf{g}_2) < d.$$

С другой стороны, сумма $\mathbf{g}_1 \oplus \mathbf{g}_2$ обязательно приналежит G. Поэтому $||\mathbf{g}_1 \oplus \mathbf{g}_2|| \geq d$. Пришли к противоречию. Теорема доказана.

Теорема 1.1 является частным случаем следующего более общего утверждения об ошибках, исправляемых линейными кодами

Теорема 1.2 *В линейном коде множества исправляемых ошибок всех элементов совпадают.*

ДОКАЗАТЕЛЬСТВО. Допустим, что теорема не верна, и в каком-нибудь линейном коде G найдутся такие два элемента $\mathbf{g}_1$ и $\mathbf{g}_2$, что вектор с принадлежит множествуисправляемых ошибок элемента $\mathbf{g}_1$ и не принадлежит множествуисправляемых ошибок элемента $\mathbf{g}_2$. Тогда для вектора $\mathbf{g}_1 \oplus \mathbf{c}$ ближайшим элементом кода будет $\mathbf{g}_1$, а для вектора $\mathbf{g}_2 \oplus \mathbf{c}$ найдется элемент кода $\mathbf{g}_3$, расстояние до которого не меньше, чем до $\mathbf{g}_2$. Следовательно, существует вектор $\mathbf{c}'$ такой, что $\mathbf{g}_2 \oplus \mathbf{c} \oplus \mathbf{c}' = \mathbf{g}_3$ и $||\mathbf{c}'|| \leq ||\mathbf{c}||$. Но тогда вектор $\mathbf{c} \oplus \mathbf{c}' = \mathbf{g}_2 \oplus \mathbf{g}_3 = \mathbf{g}_4$ является элементом кода G. Поэтому расстояние от вектора $\mathbf{g}_1 \oplus \mathbf{c} = \mathbf{g}_1 \oplus \mathbf{g}_4 \oplus \mathbf{c}$ до элемента $\mathbf{g}_1 \oplus \mathbf{g}_4$ не меньше, чем расстояние до $\mathbf{g}_1$, т. е. вектор $\mathbf{c}$ не принадлежит множествуисправляемых ошибок элемента $\mathbf{g}_1$. Полученное противоречие показывает, что множества исправляемых ошибок всех элементов совпадают. Теорема доказана.

Теорема 1.2 позволяет говорить о множестве ошибок, исправляемых линейным кодом. Пусть линейный код G исправляет ошибки из множества C. Повторяя доказательство теоремы 1.2, нетрудно показать, что

$$\mathbf{c}_i \oplus \mathbf{c}_j \notin G \text{ для всех } \mathbf{c}_i, \mathbf{c}_j \text{ из } C. \tag{1.1}$$

Действительно, если в C найдутся такие $\mathbf{c}_i$ и $\mathbf{c}_j$, что $\mathbf{c}_i \oplus \mathbf{c}_j \in G$, то для каждого из этих векторов найдется по крайней мере два ближайших элемента кода — нулевой и $\mathbf{c}_i \oplus \mathbf{c}_j$.

Булева (k, n)-матрица $\mathbf{G}$ называется *порождающей* матрицей линейного кодаG, если линейная оболочка $\langle \mathbf{g}_1, \ldots, \mathbf{g}_k \rangle$ строк матрицы $\mathbf{G}$ совпадает с G. При помощи порождающей матрицы $\mathbf{G}$ очень просто выполняется процедура кодирования: для преобразования информационного вектора $\mathbf{a}$ длины k в кодовое слово $\mathbf{g}$ длины n достаточно вычислить произведение $\mathbf{aG}$.

Булева $(n-k, n)$-матрица $\mathbf{H}$ называется *проверочной* матрицей линейного кода G, если $\mathbf{Hg} = \mathbf{0}$ для каждого $\mathbf{g} \in G$ и $\mathbf{Hx} \neq \mathbf{0}$ для каждого $\mathbf{x} \notin G$. Вектор $\mathbf{Hx}$ называется *синдромом* вектора $\mathbf{x}$ и обозначается символом S. Нетрудно видеть, что $\mathbf{Hc_i} \neq \mathbf{Hc_j}$ для любых исправляемых кодом G ошибок $\mathbf{c_i}$ и $\mathbf{c_j}$, так как в противном случае $\mathbf{H}(\mathbf{c_i} \oplus \mathbf{c_j}) = \mathbf{0}$ и, следовательно, $\mathbf{c_i} \oplus \mathbf{c_j} \in G$, что, очевидно, невозможно. Таким образом, справедлива следующая теорема.

Теорема 1.3 *Для того, чтобы матрица* $\mathbf{H}$ *была проверочной матрицей кода, исправляющего ошибки из множества* C*, необходимо и достаточно, чтобы* $\mathbf{Hc_i} \neq \mathbf{Hc_j}$ *для любых ошибок* $\mathbf{Hc_j}$ *и* $\mathbf{Hc_j}$ *из* C*.*

Отметим, что

$$\mathbf{H}(\mathbf{g} \oplus \mathbf{c}) = \mathbf{H}(\mathbf{g}) \oplus \mathbf{H}(\mathbf{c}) = \mathbf{H}(\mathbf{c})$$

для любого элемента кода $\mathbf{g}$ и любого вектора ошибок $\mathbf{c}$. Поэтому вычисление синдрома может существенно упростить декодирование по сравнению с общим нелинейным случаем. Для декодирования набора $\mathbf{x}$ надо вычислить его синдром и затем сравнить полученный результат с заранее вычисленными синдромами векторов ошибок. Такое декодирование называется синдромным и его сложность (без учета сложности вычисления синдрома) есть $n2^n - k$. Эту величину можно значительно уменьшить при помощи метода согласования, успешно работающего в различных ситуациях. Опишем этот метод.

Пусть линейный (n, k)-код G исправляет t ошибок. Допустим, что при передаче вектора $\mathbf{g}$ произошло не более t ошибок, и был получен вектор $\mathbf{x}$. Пусть $\mathbf{c}$ — вектор ошибок, т. е. $\mathbf{g} \oplus \mathbf{c} = \mathbf{x}$. Пусть A — множество синдромов $S(\mathbf{c}_l)$ всех векторов ошибок $\mathbf{c}_l$, вес которых не превосходит $\lceil t/2 \rceil$, B — множество попарных сумм синдрома $S(\mathbf{x})$ принятого вектора $\mathbf{x}$ и синдромов $S(\mathbf{c}_m)$ всех векторов ошибок $\mathbf{c}_m$, вес которых не превосходит $\lfloor t/2 \rfloor$. Так как любой вектор, вес которого не превосходит t, можно представить в виде суммы двух векторов, вес первого из которых не превосходит $\lceil t/2 \rceil$, а второго — $\lfloor t/2 \rfloor$, то, очевидно, что найдутся такие векторы $\mathbf{c}_i$ и $\mathbf{c}_l$, что $\mathbf{c} = \mathbf{c}_i \oplus \mathbf{c}_j$, где $||\mathbf{c}_i|| \leq \lceil t/2 \rceil$ и $||\mathbf{c}_j|| \leq \lfloor t/2 \rfloor$. Поэтому в силу линейности синдрома

$$S(\mathbf{x}) = S(\mathbf{c}) = S(\mathbf{c}_i \oplus \mathbf{c}_j) = S(\mathbf{c}_i) \oplus S(\mathbf{c}_j)$$

Переписав последнее равенство в виде $S(\mathbf{x}) = S(\mathbf{c}_i) \oplus S(\mathbf{c}_j)$, заключаем, что существует непустое пересечение множеств A и B, и если в этих множествах найти пару одинаковых элементов, то по этой паре можно будет восстановить вектор ошибок. Найти такую пару можно следующим образом. Сначала вычислим все синдромы из множества A и все суммы из множества B. Затем упорядочим множество A. После этого последовательно для каждого элемента из B попробуем найти равный ему элемент из A. Если такой элемент есть, то его можно найти, выполнив не более $\lceil log_2|A| \rceil$ сравнений текущего элемента из B с элементами из A. Сначала элемент из B сравнивается со средним элементом из A. Если элемент из B окажется меньше, то далее поиск ведется в первой половине A, если больше — во второй половине A. Если в A есть элемент, равный текущему элементу из B, то он будет обнаружен во время одного из сравнений. Нетрудно видеть, что для декодирования вектора $\mathbf{x}$ достаточно выполнить

$$\mathcal{O}(|B|log_2|A|) = \mathcal{O}\left(\left(\sum_{i=0}^{\lfloor t/2 \rfloor} \binom{n}{i}\right) log_2 \sum_{i=0}^{\lceil t/2 \rceil} \binom{n}{i}\right) = \mathcal{O}\left(2^{nH(t/2n)} nH(t/2n)\right) \tag{1.2}$$

операции над векторами длины $n - k$.

В следующей теореме устанавливается фундаментальное свойство линейных кодов, лежащее в основе подавляющего числа конструкций этих кодов.

Теорема 1.4 *Для того, чтобы матрица* $\mathbf{H}$ *была проверочной матрицей линейного кода с кодовым расстоянием не меньшим* d *необходимо и достаточно, чтобы любые* $d-1$ *столбцов матрицы* $\mathbf{H}$ *были линейно независимы.*

ДОКАЗАТЕЛЬСТВО. Установим необходимость. Пусть $\mathbf{H}$ — проверочная матрица кода G с расстоянием d. Если в матрице $\mathbf{H}$ сумма столбцов с номерами $i_1, \ldots, i_l$ равна нулевому вектору, то произведение $\mathbf{Hv}$ матрицы $\mathbf{H}$ и вектора $\mathbf{v}$, у которого единичные компоненты имеют номера $i_1, \ldots, i_l$, также будет равно нулевому вектору. Следовательно, вектор $\mathbf{v}$ принадлежит G, и, поэтому, $l \geq d$. С другой стороны, если любые $d-1$ столбцов матрицы $\mathbf{H}$ линейно независимы, то и произведение матрицы $\mathbf{H}$ и любого вектора $\mathbf{v}$ с не более чем $d-1$ единичными компонентами не равно нулевому вектору, и в силу теоремы 1.1 нулевое пространство матрицы $\mathbf{H}$ будет кодом с расстоянием не меньшим d. Теорема доказана.

Докажем нижнюю оценкудля мощности максимальных линейных кодов, исправляющих данное число ошибок. Эта оценка называется неравенством Варшамова–Гилберта.

Теорема 1.5 *Если числа* n, m *и* d *удовлетворяют неравенству*

$$2^{n-m} > \sum_{i=0}^{d} -2 \binom{n-1}{i},$$

то существует линейный (n, m)*-код с расстоянием* d.

ДОКАЗАТЕЛЬСТВО. Допустим, что найдется матрица $\mathbf{H}_k$ из $n-m$ строк и k столбцов, у которых любые $d-1$ столбцов линейно независимы. Тогда существует не более $\sum_{i=0}^{d-2} \binom{k}{i}$ различных линейных комбинации столбцов этой матрицы, в каждую из которых входит не более чем $d-2$ ненулевых слагаемых. Если $2^{n-m} > \sum_{i=0}^{d} -2 \binom{k}{i}$, то найдется хотя бы один ненулевой вектор $\mathbf{h}$ длины $n-m$, не совпадающий ни с одной из этих линейных комбинации. Нетрудно видеть, что в матрице $\mathbf{H}_k + 1 = (\mathbf{H}_k \mathbf{h})$, составленной из столбцов матрицы $\mathbf{H}_k$ и вектора $\mathbf{k}$, любые $d-1$ столбцов линейно независимы, и в силу теоремы 1.4 эта матрица будет проверочной матрицей кода с расстоянием d. Теорема доказана.

Так как синдромы всех исправляемых линейными (n, m)-кодом ошибок различны, то неравенство $n - m \geq \lceil log_2 \sum_{i=0}^{t} \binom{n}{i} \rceil$ справедливо для любого такого кода, исправляющего t ошибок. Объединив это неравенство с границей Варшамова–Гилберта, для мощности максимального линейного (n, m)-кода G, исправляющего t ошибок, получим двойное неравенство

$$\frac{2^n}{\sum_{i=0}^{2t-1} \binom{n}{i}} \leq |G| = 2^m \leq 2^{n - \lceil log_2 \sum_{i=0}^{t} \binom{n}{i} \rceil} \leq \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}} \tag{1.3}$$

являющееся аналогом неравенства (13.7) для произвольных кодов. Заметим, что нижняя оценка в 1.3 немного усиливает нижнюю оценку в (13.7). Однако это усиление не столь велико, чтобы существенно улучшить оценки скорости линейных кодов по сравнению с аналогичными оценками (13.8) и (13.9). Как и в случае произвольных кодов нетрудно показать, что для скорости максимального линейного кода длины n, исправляющего t ошибок, справедливы неравенства

$$1 - H\left(\frac{2t}{n}\right) \leq R \leq 1 - H\left(\frac{t}{n}\right) + \mathcal{O}\left(\frac{log_2 n}{n}\right) \tag{1.4}$$

и что при помощи линейных кодов по двоичному симметричному каналу с вероятностью ошибки p можно передавать информацию с близкой к нулю вероятностью неправильного декодирования и скоростью

$$1 - H((1 + \delta)2p) \leq R \leq 1 - H((1 + \delta)p) \tag{1.5}$$

где δ — сколь угодно малое положительное число, удовлетворяющее неравенству $1 - H((1 + \delta)2p) \leq 1/2$