НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

Модуль 2. Линейные блоковые коды

Определение линейных блоковых кодов через порождающую и проверочную матрицы. Канонические формы матриц. Кодирование линейным кодом.

Иванов Ф. И.
к.ф.-м.н., доцент

Национальный исследовательский университет
«Высшая школа экономики»

12 июня 2020 г.

Линейный и групповой код

Рассмотрим задачу построения кодов, заданных над полем $GF(q^m)$, q — простое, $m \in \mathbb{N}$.

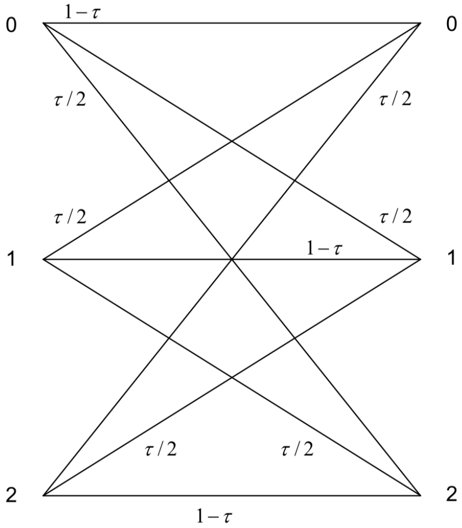
Определение

Код A называется линейным (n,k)-кодом, если он является некоторым k-мерным подпространством линейного пространства V векторов длины n над полем $GF(q^m)$: из $\mathbf{a},\mathbf{b} \in A$, $\alpha,\beta \in GF(q^m)$ следует, что $\alpha\mathbf{a} + \beta\mathbf{b} \in A$.

Определение

Если $m = 1$, то $GF(q^m) = GF(q)$ и V над полем $GF(q)$ является группой. Тогда подгруппа A группы V над $GF(q)$ называется групповым кодом. Так как порядок V есть q^n, то порядок A есть q^k, где $k < n$.

q-ичный симметричный канал - Пример $q = 3$



q-ичный симметричный канал - общий случай

- q входов: $X = \{0,1,...,q-1\}$
- q выходов: $Y = \{0,1,...,q-1\}$
- Вероятность перехода одинакова для всех символов:

$$P(y \neq x) = P(y \neq x : y \in Y, x \in X) = \frac{\tau}{q-1},$$

  где τ — вероятность искажения символа
- Вероятность ошибки:

$$P_{err} = \sum_{y} P(y \neq x) = \tau$$

- Вероятность правильной передачи символа:

$$P_{corr} = 1 - P_{err} = 1 - \tau$$

Порождающая матрица линейного кода

- Размерность V: $\dim V = n$, а значит его базис состоит из n векторов, например $\mathbf{e}_1$, $\mathbf{e}_2$, ..., $\mathbf{e}_n$, где $\mathbf{e}_i$ — единичные орты
- Размерность A: $\dim V = k$, а значит его базис состоит из k векторов $\mathbf{a}_1$, $\mathbf{a}_2$, ..., $\mathbf{a}_k$ длины n. Это значит, что любой вектор $\mathbf{c} \in A$ имеет вид:

$$\mathbf{c} = \alpha_1 \mathbf{a}_1 + \alpha_2 \mathbf{a}_2 + \ldots + \alpha_k \mathbf{a}_k,$$

где $\alpha_i \in GF(q)$.

Составим $k \times n$ матрицу $\mathbf{G}$, называемую порождающей матрицей кода A:

$$\mathbf{G} = \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \cdots \\ \mathbf{a}_k \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & a_{k3} & \ldots & a_{kn} \end{pmatrix}$$

Кодирование линейным кодом

Задача: для данного информационного вектора $\mathbf{u} = (u_1, u_2, ..., u_k)$, $u_i \in GF(q)$ найти соответствующий ему кодовый вектор $\mathbf{c} \in A$.
Очевидно, что:

$$u_1\mathbf{a}_1 + u_2\mathbf{a}_2 + ...u_k\mathbf{a}_k = \mathbf{c} \in A$$

Как записать это в терминах порождающей матрицы?

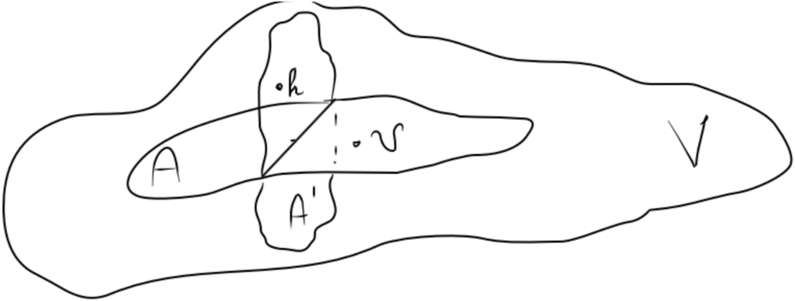
$$(u_1, u_2, ..., u_k)\begin{pmatrix}\mathbf{a}_1\\ \mathbf{a}_2\\ \dots\\ \mathbf{a}_k\end{pmatrix} = u_1\mathbf{a}_1 + u_2\mathbf{a}_2 + ...u_k\mathbf{a}_k = \mathbf{c},$$

$$\mathbf{c} = \mathbf{uG}$$

Причем так как $\mathbf{G}$ — матрица полного ранга k, то отображение взаимно-однозначно!

Ортогональное подпространство

Наряду с подпространством $A \subset V$ рассмотрим такое подпространство $A' \subset V$, что B содержит в точности q^{nk} векторов, и для любой пары векторов $\mathbf{v} \in A, \mathbf{h} \in A'$ скалярное произведение $(\mathbf{v},\mathbf{h}) = 0$. Подпространства $A \subset V$ и $A' \subset V$ называются взаимно ортогональными.



Проверочная матрица линейного кода

Ортогональное подпространство состоит из q^{n-k} векторов, а значит его базис состоит из $n-k$ векторов длины n:

$$\mathbf{h}_1, \mathbf{h}_2, ..., \mathbf{h}_{n-k}.$$

Причем $\forall \mathbf{v} \in A : (\mathbf{v}, \mathbf{h}_i) = 0$. По аналогии с $\mathbf{G}$ построим порождающую матрицу подпространства A':

$$\mathbf{H} = \begin{pmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \dots \\ \mathbf{h}_{n-k} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \dots & h_{1n} \\ h_{21} & h_{22} & h_{23} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ h_{n-k,1} & h_{n-k,2} & a_{n-k,3} & \dots & a_{n-k,n} \end{pmatrix}$$

Данную матрицу называют проверочной матрицей линейного кода, так как

$$\mathbf{v} \in A : \mathbf{H}\mathbf{v}^T = \begin{pmatrix} (\mathbf{v}, \mathbf{h}_1) \\ (\mathbf{v}, \mathbf{h}_2) \\ \dots \\ (\mathbf{v}, \mathbf{h}_{n-k}) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix} = \mathbf{0}$$

2 определения линейного кода

Линейный код A полностью определяется своей порождающей или проверочной матрицами. Можно дать 2 альтернативных описания линейного кода:

$$A = \{\mathbf{c} \in V : \mathbf{c} = \mathbf{uG}, \forall \mathbf{u} = (u_1, u_2, ... u_k)\} \quad (1)$$

$$A = \{\mathbf{c} \in V : \mathbf{cH}^T = \mathbf{0}\} \quad (2)$$

Способ (1) удобен при кодировании, способ (2) удобен при декодировании.
Имеется связь между **G** и **H**:

$$\mathbf{GH}^T = \mathbf{0}_{k \times (n-k)}$$

Матрицы **G** и **H** называют базисными матрицами линейного кода A.

Каноническая форма базисных матриц

Идея: выделить в матрице **G** единичную подматрицу.
Шаги:

1. В i-й строке $(i = 1,2,\dots,k)$ матрицы **G** найдется по крайней мере одна ненулевая компонента. Пусть первая отличная от нуля компонента этой строки находится в j-м столбце. Разделим каждую компоненту строки на a_{ij}. В результате получится новая компонента a'_{ij} матрицы, равная единице.
2. К каждой z-й строке $(z \neq i)$ прибавим i-ю строку, умноженную на a_{zj}. В результате в j-м столбце i-я строка будет содержать единицу, а все остальные строки — нули.
3. Применим шаги (1)-(2) к каждой строке матрицы **G**
4. Столбцы с одной единицей переставим на первые k позиций.

В результате получим:

$$\mathbf{G}' = [\mathbf{I}_{k\times k} \;\; \mathbf{P}_{k\times(n-k)}],$$

Пример построения канонической матрицы

Пусть имеем порождающую матрицу (7,4) кода:

$$G' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Прибавим к первой строке вторую, а к третьей — четвёртую. Новая матрица будет:

$$G'' = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Матрицы $\mathbf{G}'$ и $\mathbf{G}''$ порождают одно и то же подпространство, так как одна из другой получены элементарными операциями. Если теперь в $\mathbf{G}''$ поменять местами четвёртый и седьмой столбцы, получим матрицу:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & : & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & : & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & : & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & : & 0 & 1 & 1 \end{bmatrix}$$

Кодирование при канонической форме порождающей матрицы

Легко заметить, что кодирование посредством матрицы **G** в канонической форме сохраняет все символы вектора $u = (u_1, u_2, \ldots, u_k)$ длины k в качестве первых k символов кодового вектора. Эти символы называют информационными символами. Остальные $n - k$ символов называются проверочными и (или) избыточными.

Пример

Пусть $\mathbf{u} = (1001)$*. Закодируем его при помощи матрицы* $\mathbf{G}$*, полученной в предыдущем примере. Тогда:*

$$\mathbf{c} = \mathbf{uG} = (1001110).$$

Легко заметить, что

$$\mathbf{c} = (\mathbf{up}),$$

где $\mathbf{p} = (110)$ *— проверочные символы*

Каноническая форма проверочной матрицы

Теорема

Если

$$\mathbf{G}_K = [\mathbf{I}_{k\times k} \quad \mathbf{P}_{k\times(n-k)}]$$

есть каноническая форма порождающей матрицы, то каноническая форма проверочной матрицы есть

$$\mathbf{H}_K = [-\mathbf{P}^T_{(n-k)\times k} \quad \mathbf{I}_{(n-k)\times(n-k)}]$$

Пример

В приведенном выше примере получим:

$$H = \left[\begin{array}{cccccccc} 0 & 1 & 1 & 0 & : & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & : & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & : & 0 & 0 & 1 \end{array}\right]$$

Основная теорема о минимальном расстоянии линейного кода

Определение

Весом $w(\mathbf{v})$ *вектора* $\mathbf{v}$ *называется число отличных от нуля его компонент.*

Теорема

Любому значению расстояния $d(\mathbf{v}_1, \mathbf{v}_2)$ *между векторами* $\mathbf{v}_1$ *и* $\mathbf{v}_2$ *линейного* (n,k)*-кода отвечает кодовый вектор* $\mathbf{v}_1 - \mathbf{v}_2 = \mathbf{v}$*, для веса* $w(\mathbf{v})$ *которого выполняется равенство* $w(\mathbf{v}) = d(\mathbf{v}_1, \mathbf{v}_2)$*. И, наоборот, каждому значению* $w(\mathbf{v})$ *веса кодового вектора* $\mathbf{v}$ *отвечает пара кодовых векторов* $\mathbf{v}_1$ *и* $\mathbf{v}_2$ *с расстоянием* $d(\mathbf{v}_1, \mathbf{v}_2) = w(\mathbf{v})$*, причём таких пар имеется в точности* q^k*.*

Доказательство основной теоремы

В силу того, что код — всегда группа с операцией поразрядного сложения векторов, разность двух кодовых векторов есть снова кодовый вектор: $\mathbf{v}_1 - \mathbf{v}_2 = \mathbf{v}$, и вес $w(\mathbf{v})$ вектора $\mathbf{v}$, т.е. число отличных от нуля его компонент в точности равно расстоянию $d(\mathbf{v}_1, \mathbf{v}_2)$. Наоборот, пусть вектор $\mathbf{v}$ имеет вес $w(\mathbf{v})$. Сложив вектор $\mathbf{v}$ с произвольным кодовым вектором $\mathbf{v}_i$, получим, что $d(\mathbf{v} + \mathbf{v}_i, \mathbf{v}_i) = w(\mathbf{v})$, чем и завершается доказательство. Остаётся вспомнить, что кодовых векторов $\mathbf{v}_i$ имеется в точности q^k.

Метрические свойства проверочной матрицы

Пусть $\mathbf{v} = (a_1, a_2, \ldots, a_n)$ — кодовый вектор. Представим проверочную матрицу в виде

$$\mathbf{H} = [\mathbf{h}_1\ \mathbf{h}_2\ \ldots \mathbf{h}_n],$$

где $\mathbf{h}_i$ есть i-й вектор-столбец проверочной матрицы. Тогда выражение $\mathbf{vH}^T = \mathbf{0}$ можно переписать в виде:

$$a_1\mathbf{h}_1 + a_2\mathbf{h}_2 + \ldots + a_n\mathbf{h}_n = \mathbf{0}.$$

Иначе говоря, каждый отличный от нуля кодовый вектор $\mathbf{v}$ задаёт нетривиальное соотношение линейной зависимости векторов-столбцов проверочной матрицы. Пусть $a_{i_1}, a_{i_2}, \ldots, a_{i_w}$ все отличные от нуля компоненты вектора $\mathbf{v}$. Тогда равенство превратится в

$$a_{i_1}\mathbf{h}_{i_1} + a_{i_2}\mathbf{h}_{i_2} + \ldots + a_{i_w}\mathbf{h}_{i_w} = \mathbf{0}.$$

Если $w \leq d - 1$, то это означает, что имеется такой кодовый вектор, вес которого не превосходит $d - 1$, а значит, найдутся такие пары векторов, расстояния между которыми не превос- ходит $d - 1$. Тем более, минимальное расстояние оказывается меньше чем d. С другой стороны, если любые $d - 1$ столбцов проверочной матрицы линейно независимы, то минимальный вес, а значит минимальное расстояние кода, не менее d.

Основная теорема о проверочной матрице

Теорема

Для того, чтобы минимальное расстояние линейного кода было не менее, чем d, необходимо и достаточно, чтобы любые $d-1$ и менее столбцов проверочной матрицы были линейно независимы.

Следствие

Граница Синглтона

$$d-1 \leq n-k.$$

Граница Варшамова-Гилберта

Будем строить проверочную матрицу $\mathbf{H}$ размера $(n-k) \times n$ следующим образом. В качестве первого столбца $\mathbf{h}_1$ можно выбрать любой ненулевой столбец длины $n-k$. Вторым столбцом$\mathbf{h}_2$ может стать любой из оставшихся $q^{n-k}-q$ столбцов, кроме нулевого и $q-1$ столбцов, кратных столбца $\mathbf{h}_1$. Предположим, что выбрано уже j столбцов. Имеется не более

$$(q-1)\binom{1}{j}+(q-1)^2\binom{2}{j}+\ldots+(q-1)^{d-2}\binom{d-2}{j}$$

их различных линейных комбинаций, содержащих $d-2$ и менее столбцов. Если эта величина меньше, чем $q^{n-k}-1$, то можно добавить еще один ненулевой столбец, который отличен от всех этих линейных комбинаций. Тогда никакие $d-1$ столбцов из выбранных $j+1$ столбцов не будут линейно зависимы.

Граница Варшамова-Гилберта

Если выполняется соотношение

$$(q-1)\binom{1}{n-1}+(q-1)^2\binom{2}{n-1}+...+(q-1)^{d-2}\binom{d-2}{n-1} < q^{n-k}-1$$

то можно добавить еще один ненулевой nй столбец, и любые $d-1$ и менее из этих n столбцов будут линейно независимы.
Проверочная матрица построена.
У данной границы есть предельная форма:

$$R \leq 1 - h(\delta),$$

где $R = k/n$, $\delta = d/n$, $h(x)$ - функция энтропии.

Асимптотическая граница Варшамова-Гилберта