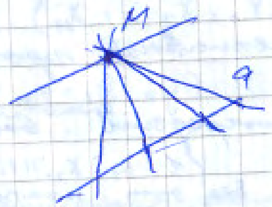
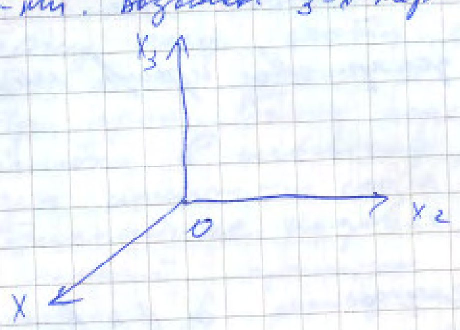
18.10.06.

Проективное пространство

Возьмем плоскость Q, проведем в ней прямую „a" и (•)-у M вне прямой. Проведем через M множество прямых пересек-х a. Каждой (•)-е пересеч. соотв. своя прямая, обратное не справедливо т.к. ||-е прямые не пересек-ся. Введем ∞-но удаленную (•)-у в кот. пересек. ||-е прямые в независимости от того в какую сторону они продолжаются. Пусть все ||-е прямые пересек. в 1-й ∞-о удал. (•)-е.



Возьмем семейство других ||-х прямых. Для них введем другую ∞-о удален. (•). Тогда вся плоскость разбив. на классы эквивалентности ||-х прямых. Назовем мн-во всех удаленных (•)-х беск-но удаленной прямой. Плоск. дополненная ∞ удал. прямой наз. проективной плоск-ю. Введем на ней СК. Обычные (•)-и выражаются через коорд-ы, а ∞ удал. (•) через пересечение прямых. Возникает неравенство м/у (•)-ми. Возьмем 3-х-мерное простр-во.



Поместим в него плоск. $x_1 = 1$. Провед. через (•)-у O множ. прямых, кот. пересек. данную плоск. тогда каждой (•)-е на пл. соотв. своя прямая.

Каноническ. ур. прямой.

$$\frac{x_1}{p_1}=\frac{x_2}{p_2}=\frac{x_3}{p_3}$$

p_1, p_2, p_3 – направл. элементы.

Если $\rho \neq 0$, то ур. прямой не изменится, если взять $\rho p_1, \rho p_2, \rho p_3$. Возьмем в кач. коорд. (•)-и на плоск. (p_1, p_2, p_3), эти коорд. опред. неоднозначно, неизменно лишь их отношение, поэтому использ-ся отношение $(p_1 : p_2 : p_3)$

Иванов

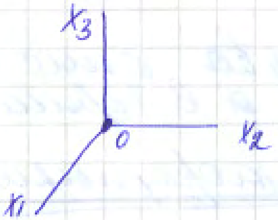
18.10.2006г.

Проективное пр-во.

Нет тупь-тупь...

Возьмем 3-х мерн. пр-во

Пл-ть $x_1 = 1$



Пров. через (.) O мн-во прямых, пер. л-ют данную пл-ть.
Тогда кажд. (.) на пл-ти соотв. своя прямая.
Канонич. ур-е прямой

$$\frac{x_1}{p_1} = \frac{x_2}{p_2} = \frac{x_3}{p_3}$$

p_1, p_2, p_3 — направляющие эл-ты

Если $\rho \neq 0$, то ур-е прямой не изменится, если взять $\rho p_1, \rho p_2, \rho p_3$

Возьмем в кач-ве коорд (.) (p_1, p_2, p_3). Коорд-ты определены неоднор-ные, неизменно лишь их отнош-е ⇒ исп-ся соотнош-е:

$$(p_1 : p_2 : p_3)$$

Это означает, что (p_1, p_2, p_3) эквив. $(\rho p_1, \rho p_2, \rho p_3)$

Т.о. пр-во разбив-ся на классы эквивал-ти одномерных подпространств — прямых (эквивал-х) проекц.

Коорд-ты точки на пл-ти определ:

$$\left(1 : \frac{p_2}{p_1} : \frac{p_3}{p_1}\right)$$

При стремлении (.) в ∞, 2-я и 3-я коорд-ы ⇒ образуют беск. удал. точку

$$(0 : p_2 : p_3)$$

Теперь все точки хар-ся проект. координат.

Если рассм. пр-во размерности n с коорд. $(x_1, x_2, \ldots, x_n)$, то его можно

вложить в проективное пр-во

$(y_0 : y_1 : y_2 : \dots : y_n)$

Непосредственно уложить можно с помощью:

$(1 : x_1 : x_2 : \dots : x_n)$

Часто проективные пр-ва описыв не в терминах координат, а в терминах мн-ва прямых.
Такие координ. наз-ся однородными

Основы теории кодирования.

Пусть A - мн-во некот-х эл-в.
$q = |A|$ - мощность мн-ва (т.е. кол-во эл-в)

A наз-ся алфавитом

Построим мн-во как декарт. произведение мн-ва A, взятое n раз

$$A^n = \underbrace{A \times A \times \dots \times A}_{n \text{ раз}}$$

Элементами A^n будут объекты вида:

$a = (a_1, a_2, \dots a_n)$

$b = (b_1, b_2, \dots, b_n)$

$a_i, b_i \in A$

Эти объекты наз-ем векторами или словами, а их компоненты - координатами или позициями.

Определим метрику пр-ва A^n как кол-во попарно несовпадающих координат векторов a и b, т.е. мн-во всех пар $a_i \neq b_i$.
Это метрика Хэмминга.
Выделим в A^n подмн-во $C \subset A^n$ с мощностью $M = |C|$
Во логарифмич. шкале $k = \log_q C$, $k \in \mathbb{N}$
C наз-ем кодом, кот-ое с парам-ми $[n, k, d]_q$
Определим тж расстояние дно Хэмминга между всеми $a, b \in C$.
q - мощность алфавита.
Также определ параметры:

$R = \frac{k}{n}$ - скорость кода

$\delta = \frac{d}{n}$ - относительное расстояние

Осн. принципы обнаружения ошибок

Пусть имеется информ-ое сообщ-е в алфавите A.
При прохожд-и его через канал в нем появл. некот-е, кот. не всегда исправляются.
Разобьем информ. сообщ. на блоки длиной k символов.
Поставим в соотв-е каждому блоку информ-го сообщ-я слово из кода C.
Был блок длиной k симв, стал блок длиной n симв.
При прохожд-и блока через канал в нем появл. ошибки в симв.
Далее решая задачу декодир-я для некот-го слова по вектор. критерию ищется ближайш. кодовое слово.
Данный принцип имеет некот-е ограничения $\Rightarrow$ нет ее упрощения и конкретизации

Цел-с теряется мн-во слишком широко ⇒ введём более конкретное понятие:

F_q – поле, где $\boxed{q = 2^m}$

Возьмём аффинное пространство F_q^n

Кол-во точек (векторов) в этом прве $= q^n$

Подпространство $C \in F_q^n$

Размерность $\dim C = k \quad k < n$

C наз-ся кодом.

Определим вес вектора (слова) $wt(a)$ как кол-во ненулевых его координат.

Код наз-ся линейным (из определения подпространства), ⇒ $\forall$ лин. комб-я 2-х кодов

$\alpha a + \beta b$

$\alpha, \beta \in F_q^*$ (мультипликативная группа поля F_q)

$a, b \in C$

также является кодовым словом из C.

⇒ нулевой вектор у.б. кодовым словом.

Код наз-ся групповым, если кодовые слова образуют группу по сложению.

Учитывая поле F_{2^m} можно утв., что хеммингово расст-е м/у словами – это вес их суммы.

В данном случ. для группового кода тт хеммингово расст-е равно тт весу слова в коде.

Введём в подпространстве C базис из k векторов длиной n:

$c_1, c_2 \dots c_k$

в координатной форме:

$C_i (C_i^{(1)}, C_i^{(2)}, \dots C_i^{(n)})$

Составим м-цу G из базисных век-в, выраж-ю в координатной форме:

$$G = \begin{pmatrix} C_1^{(1)} & C_1^{(2)} & \dots & C_1^{(n)} \\ C_2^{(1)} & C_2^{(2)} & \dots & C_2^{(n)} \\ \dots & \dots & \dots & \dots \\ C_k^{(1)} & C_k^{(2)} & \dots & C_k^{(n)} \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$$

G – порождающая м-ца кода

$c_1, c_2 \dots c_k$ – базисные векторы

Пусть имеется информационный блок

$U = (u_1, u_2, \dots, u_k)$

Выясним множ. кодов-ю базисн. век-в с коэф-ми из U.

Это и будет кодовое слово длиной n, соотв. информац-ну сообщ-ю U.

$U \cdot G$

Автоморфизмы кодов

Пусть в прве F_q^n действует группа линейных автоморфизмов, кот. заключается в перестановке координат в словах, а также в умножении их на коэф-ты из F_q^*

Эти автоморфизмы действуют и на код C. Пусть имеется подгруппа матриц A таких, что

$C' = CA$, тогда

C и C' наз-ся эквивалентными кодами ⇒ строго говоря, при рассмотрении

кода необх. учит. класс экв-х ему кодов.
Эквив. код можно получить также и применяя автоморфизмы к м-це G.

Дуальные коды (обратные)

Пусть имеем пр-во F_q^n, где $C \in F_q^n$ — код подпростр-во.
Определим его парам-ры $[n, k, d]_q$
Рассм. ортогональное дополнение $C_\perp$ к подпростр-ву C. ($\forall$ в-р $\in C_\perp \perp \forall$ в-ру из C)
$C_\perp$ также код.
Размерность $C_\perp$ $(n-k)$
min кодовое расст. для $C_\perp$ обозн. $d_\perp$
Тогда $C_\perp = [n, n-k, d_\perp]_q$
Для кода $C_\perp$ вв. базис из $(n-k)$ векторов и построим порождающую м-цу H.
Тогда получаемый код наз-ся дуальным.

$C \to G \to k \times n$ кол-во строк × кол-во столб.

$C_\perp \to H \to (n-k) \times n$

$\forall$ в-р (кодовое слово) из C $\perp$-рен $\forall$ данному в-ру из $C_\perp$ $\Rightarrow$ их скалярн. произвед-е $= \emptyset$.

$C_\ell \in C$
кодовое слово

$C_\ell \cdot H^T = 0$

0 – вектор-строка длиной $(n-k)$

$G \cdot H^T = 0$

0 – нулевая м-ца $k \times (n-k)$

$\Rightarrow$ порожд. м-цу дуальн. кода можно исп-ть для определения, явл-ся ли C_ℓ кодовым вектором из C.
Если $C_\ell H^T = 0$, то $C_\ell \in C$

Синдром

Пусть имеется код. слово $C_\ell \in C$
вв. вектор ошибки E.
Обычно ошибок немного $\Rightarrow$
E – в-р с нулями во всех позициях, кроме ошибочных.
Ошибка хар-ся номером искаж. позиции в кодов. слове и величиной ошибки.
Тогда искаж. слово $= C_\ell + E$

$$(C_\ell + E) H^T \neq 0$$

$$(C_\ell + E) H^T = \underbrace{C_\ell H^T}_{0} + E H^T = E \cdot H^T = S$$

синдром

В-р синдрома содержит в себе только инф-ю о конфигурации ошибки.

Осн. соотношение для n, k, d.

Рассм. порожд-ю м-цу дуального кода H.
Для $C_\ell \in C$ $C_\ell \cdot H^T = 0$.
Очевидно, что $\Rightarrow$ вып-ся и для кодового слова с min весом d.
Пусть это слово C_m, т.е.

$$C_m \cdot H^T = 0$$

Определим min кол-во линейно-зав-х столбцов м-цы H.

Т.к. равное соотн. выполн., то в м-це H р.б. d линейно-зависимых столбцов ⇒ $(d-1)$ столбцов линейно-независимы.
Порядок такого минора в H равен $(n-k)$
$$\Rightarrow n-k \geq d-1$$
$$\boxed{d \leq n-k+1}$$
нер-во Синглтона

Особенности исправления ошибок.

Определим, какое кол-во ошибок код будет исправлять.
Проанализируем код: запишем все код. слова в строку, начиная с нулевого кодового слова.

$$0 \quad C_1 \quad C_2 \quad \dots \quad C_{q^k-1}$$
$$E_1 \quad C_1+E_1 \quad C_2+E_1 \quad \dots \quad C_{q^k-1}+E_1$$
.

.

Очевидно, что код явл. линейным подпростр-м ⇒ подгруппа по сложению в простр-ве F_q^n явл. нормальным делителем гр-ы векторов. Разложим все мн-во вект-в в смежные классы по этому нормальному делителю.

Мощность всего мн-ва в-ров q^n
Мощность кодовых в-ров q^k
⇒ по т. Лагранжа кол-во смежных классов, явл. нормальный делитель, будет $\frac{q^n}{q^k} = q^{n-k}$

Построим все смежн. классы. Зададим в-р ориент. ошибки E_1. Прибавим этот в-р ко всем словам кода.
Выберем след. ориент. ошибку и повторим процедуру, пока все ориент. ошибки не заполнят таблицу всеми словами с ориент. ошибкой.
Если кол-во строк меньше q^{n-k}, то начинаем рассм-ть двойные ошибки.
Возможно, что все двойные ошибки уложатся в таблицу, но для ошибки какой-то кратности кол-во оставшихся строк будет недостаточным.
Вычислим для кажд. ошибки (строки) синдром.
Все синдромы для ошибок, попавших в таблицу, р.б. различны, и смежные классы не пересек-ся м/у собой.
В общ. случ. конфигураций ошибок будет q^n, а конфигур-й синдромов q^{n-k} ⇒ начиная с некот. конфиг-и ошибок синдромы начнут повторяться.
Недостающие строки в табл. смежных классов строим для таких конф. ошибок, синдромы кот-х не совп. с уже имеющимися.
⇒ Данная табл. наз-ся стандартным расположением кода.
Для кажд. эл-т столбца ошибок наз-ся лидером смежного класса.
Пусть таблица заполнена и из канала принято нек. слово. Найдем его в этой таблице.

Если оно в 1-й строке, то сигнал не искажён, если в др. строке, то слово искажено, а передавалось в канал слово лежащее в начале данного столбца.

24.10.2006г. Анализ таблицы стандартного распол-я код.

Допустим, что табл. заполнена полностью. Тогда слова, содерж. одну ошибку, нах-ся на расст. =1 от соотв. кодового слова.
Слова с 2-мя ошиб. - на расст. =2.
Определим так кол-во ошибок, кот. с пом. таблицы м.б. исправлено полностью, т.е. при k конфигурациях.
Кол-во ошибок на единицу больше исправляется лишь частично.
Обычно табл. ограничивают теми строками, кот. соотв. полностью исправляемым ошибкам, при этом кол-во ошибок выбирают из практических соображений.
При этом гов-т, что кажд. кодов. слово окружено сферой радиуса t, где t – кол-во ошибок.
Метод испр-я ошибок с пом. таблицы явл. универсальным.
Для его исп-я выч-м синдром для кажд. конфиг-и ошибки и сост. таблицу синдром — вектор ошибки.
Для принятого слова из канала выч-м синдром и, определив по табл. в-р конфиг-и ошибки E, прибавляем его к пр. слову 2^m.