Алгебраические основы теории кодирования.

В основе теории лежит понятие множества.

Множество - это совокупность объектов, объединенных по некоторому признаку.

Объекты называются эл-тами или присвоенный им порядковый номер или идентификатор.
Задается множество
1) перечислением его эл-тов,
2) указанием правила получения сов-го эл-та по известным имеющимся.

Отображение множеств

Пусть A и B - множества. Существует 3 возможных способа отображения A в B. A - прообраз, B - образ:

1) Сюръекция: каждому образу B соответствует хотя бы один прообраз A
2) Инъекция: двум прообразам A (различным) соотв различные образы B
3) Биекция: взаимно однозначное соответствие.

Основной параметр множества - его мощность |A| - кол-во элементов в множестве.

Алгебры

Пусть на множестве определена ф-ция, которая принимает значения на этом же множестве. При этом говорят, что на множестве определена операция, набор называется алгеброй.

Наиболее распространенные алгебры, на которых определены одна или две операции одновременно. При этом двум эл-там множества ставится в соответствие третий

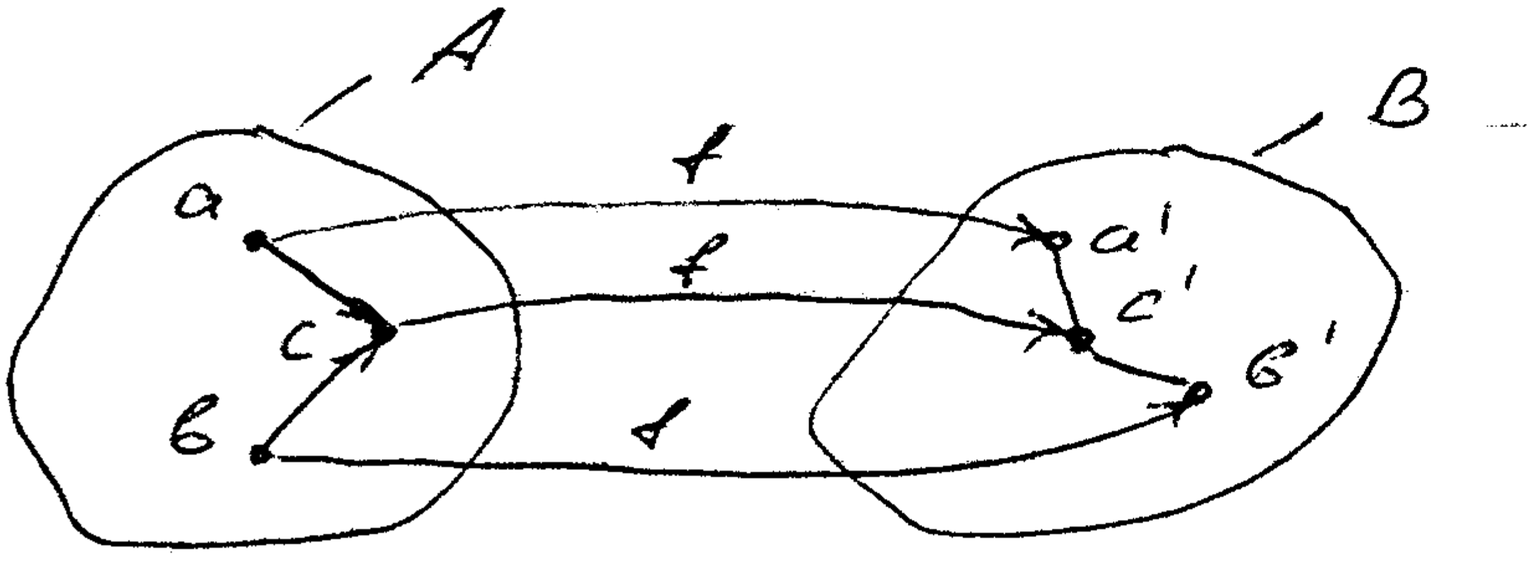
Операции обычно называют словами и символами

Изоморфизм. Гомоморфизм.

Будем рассм множества с одной операцией.

A и B - множества

Рассм. взаимнооднозн. отображение A в B, при котор операция внутр в A сохран и в B.



c - внутренняя операция, принад. A

c' - внутренняя операция, принад B

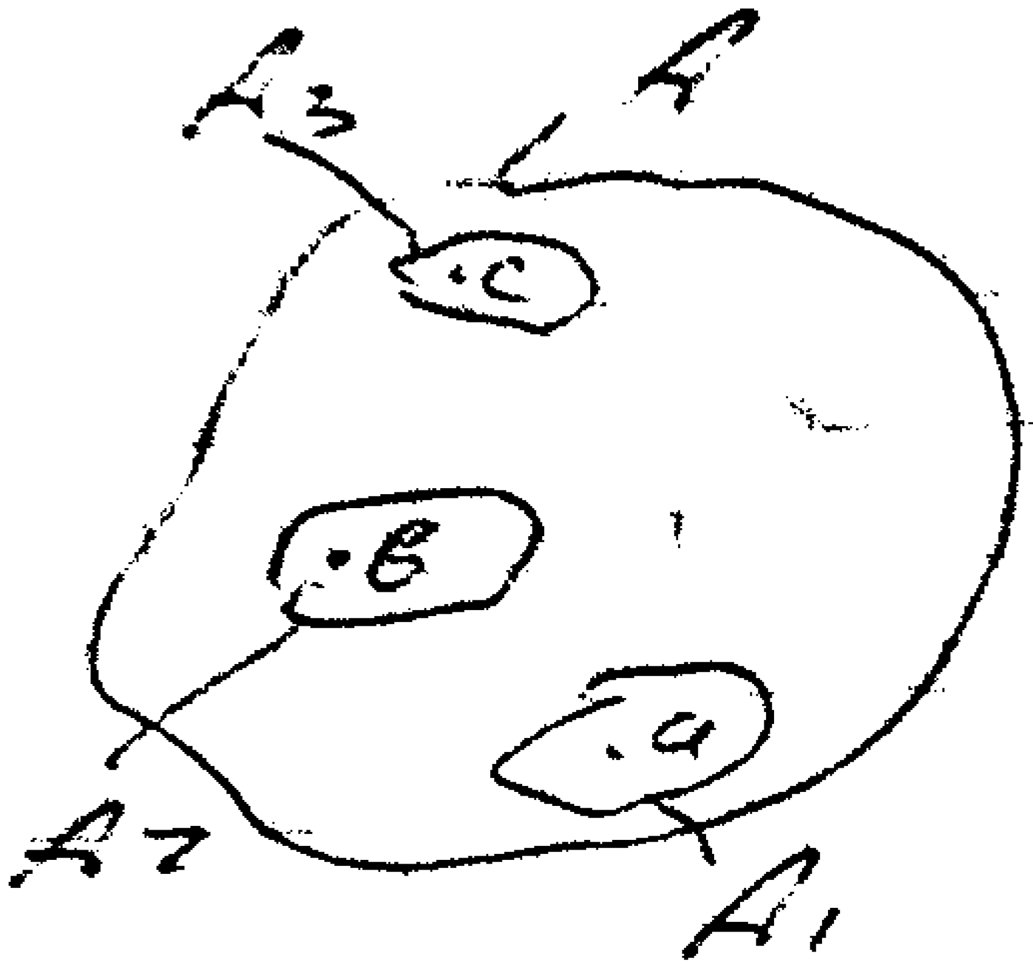
Такое отображение называется изоморфизмом

С точки зр. т-ии зрения изоморфные объекты - это копии одного и того же объекта

Пусть отображение не взаимнооднозначно, но операция сохраняется. Такое отображение гомоморфизм.

Разбиение множеств

В общем случае при гомоморфном отображении множеств A можно разбить на отдельные подмножества, каждое из которых имеет свой образ в B.



Пусть $a \in A_1$
$b \in A_2$
$c \in A_3$
Причем c – результат применен. операции к a и b

Возьмем др. эл-ты в A_1 и A_2. Допустим, что независимо от их выбора результат операции располаг. в A_3. Тогда разбиение множества – правильное. При правильном разбиении все множество распадается на непересек. подмножества, котор. сами образуют новые множества. Они назыв. фактор-множеством A по данному ~~разб~~ разбиению.

Обозначим эл-т в множестве как нейтральный(e), если для $a \in A$. $a \circ e = e \circ a = a$.
Обычно под операцией понимают умножение. При этом $e = 1$.
Если существуют левые и правые единицы e, то они равны
При операциях сложения нейтральный элемент – ноль

Пусть A_k – подмножество образ которого нейтральный элемент. Тогда это подмножество – ядро гомоморфизма.

Теорема о гомоморфизме

Пусть φ — гомоморфизм $A \times B$. При этом B будет изоморфно фактор-множеству $\bar{A}$. Тогда можно определить изоморфизм $\psi: B \to \bar{A}$, при котором совместное применение $\psi \circ \varphi$ отобразит A в $\bar{A}$.
Данное отображение является естественным гомоморфизмом.
При естественном гомоморфизме произвольному эл-ту в A ставится в соотв. подмножество, полученное при упомянутом разбиении, которое называется классом.

Группоиды.

Пусть на множестве определена одна операция (сложение или умножение)

$a \circ b = c$.

Данное множество называется группоидом.
Если $a \circ b = b \circ a$, то такой группоид называется коммутативным.
Если операция в группоиде ассоциативна, т.е. $a \circ b \circ c = (a \circ b) \circ c = a \circ (b \circ c)$, то такой группоид — полугруппа.
Если к тому же определен единичный эл-т, то группоид — полугруппа с единицей или моноид.

Определим в алгебре такой эл-т a^{-1}, что

$a^{-1}a = aa^{-1} = e$. Тогда a^{-1} — обратный эл-т к a.

Пусть полугруппа с единицей имеет для каждого эл-та обратный, тогда это группа

Пусть отображение гомоморфно группы
образом является данная группа.

Подгруппы.

Пусть в группе G имеется подмножество G_1
замкнутое относительно групповой операции
т.е. G_1 само является группой.
Для проверки G_1 как подгруппы достаточно проверить выполнение операции для
всех x-тов $a^{-1} \in G_1$.

Существует 2 тривиальные подгруппы
- единичная, содержащая только e,
- вся группа.

Если кол-во x-тов в группе конечно, то она
конечная, иначе - бесконечная.

Порядок конечной группы называют число
ее x-тов.

Верно ли любая подгруппа в группе также
является подгруппой

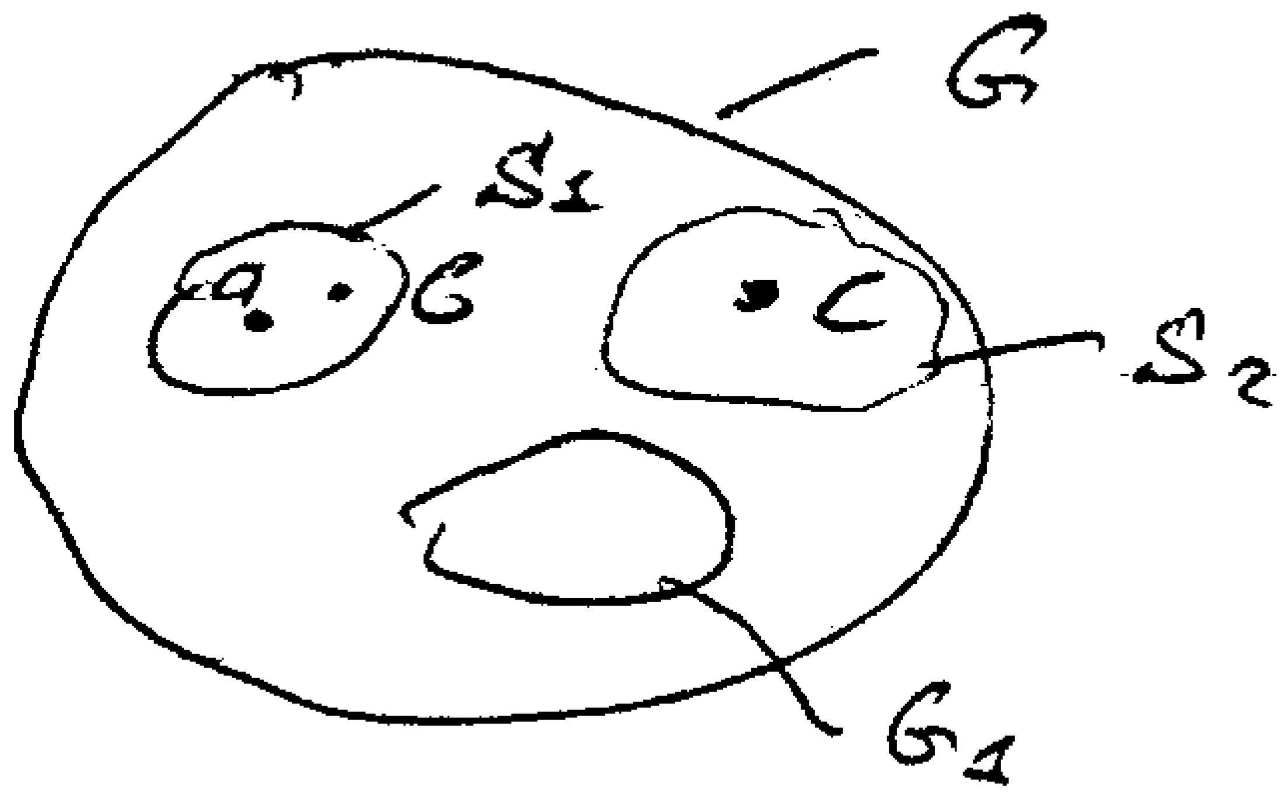
Пусть в группе имеется множество M
Найдем пересечение всех подгрупп, содержащих
M. Получим минимальную подгруппу, содержащую
M. Где M - система образующих
данной минимальной подгруппы
В данную подгруппу входят все x-ты M, степени
x-тов M (как результат применения операции
умножения), а также произведения вида $a^k b^e$,
$a, b \in M$

Особый случай, если M состоит из одного x-та.
Этот x-т называется порождающим, а все
x-ты всей подгруппы являются степенями
этого x-та

Такая группа - циклическая группа.
Если все степени образующ. эл-та a различны, то говорят, что он имеет бесконечный порядок. Пусть существует такое n, что $a^n = e$.
Тогда говорят, что a имеет порядок n.
Различны только эл-ты: $e, a, a^2, \ldots, a^{n-1}$. Это циклическая группа конечного порядка.

Разложение по подгруппе.

Пусть группа G, G_1 - подгруппа; $a \in G$; $a \notin G_1$



Реализуем всевозможные произведения a на эл-ты из G_1. Получим множество той же мощности, что и G_1, которое называется левым смежным классом S_1

Пусть $b \in S_1$, причем $b \neq a$
Рассм пр-ние bG_1. Получим тот же класс
т.е. $aG_1 = bG_1$.
~~[illegible]~~ Смежный левый класс однозначно опр-ся любым своим элементом.

Пусть $c \in G$; $c \notin G_1$, $c \notin G_1$.

Реализуем пр-ие $cG_1 = S_2$
S_2 ~~[illegible]~~ и S_1 не пересекаются

Т.о. всю группу можно разбить на левые смежные классы по подгруппе G_1.

Рассмотрим аналогичную ситуацию, в которой реализуется пр-ние вида $G_1 a$. Тогда получим разбиение группы на правые смежные классы по подгруппе G_1.
В общем случае они не совпадают, но их кол-во одинаково

Кол-во смежных классов называется индексом подгруппы j.
Пусть k - порядок G_1. Тогда порядок G:
$$n = jk.$$
Т.е. порядок подгруппы обязат-но делит порядок группы (теорема Лагранжа).

Нормальный делитель.

Пусть в группе G существ такая подгрупп H, что при разложении левые и правые смежные классы совпадают.
Т.е. $aH = Ha$.
Тогда для каждого $a \in G$, $a \notin H$ и $h \in H$ найдутся такие h', $h'' \in H$, что $ah = h'a$ и $ha = ah''$.
H - нормальный делитель, или инвариантная подгруппа.

Разбиение группы по нормальному делителю является фактор-множеством группы и обозначается G/H.

Разбиение группы G по подгруппе H является правильным, поэтому для групп справедливы теоремы об гомоморфизмах. Здесь ядрами гомоморфизмов являются ядра делителей и только они поэтому все возможн. гомоморфизмы групп можно описать, рассмотрев все существующие нормальные делители.
Нормальные делители часто опр-ся через сопряженные эл-ты. Эл-т b сопряжен a, если существ $g \in G$, что $b = g^{-1}ag$. b получается трансформацией a с помощью g.

$ha = ah'' \quad | \cdot a^{-1}$

$a^{-1}ha = h''$, т.е. нормальный делитель наряду со своими делителями содержит и все сопряженные.

Иванов Семинары.

Конечные

Обозначение конечных полей (поля Галуа)

$GF(q^n)$; q - основание поля
n – степень расширения

Простейшее поле Галуа: 0, 1, 2, 3, 4, 5, 6.
В нем опер сложения и умножение по модулю $\neq$:

$$a \cdot b \bmod m = \text{rest } \frac{a \cdot b}{m}$$

Для него опред табл сложения

т.е. $GF(7)$

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Простейшее расширение данного поля.

x^2+5x+3 – не имеет корней в поле Δ

При делении всякого полин на исходный, все полиномы разлив. на классы, в кот имеют одинак. остаток от деления

Далее образуется мульт группа, если берется элемент x, присоед. к-рого прошло расшир поля.

Т.е. расшир. с помощью одного эл-та, то мультип. группа поля получится циклической.

Сказали, что x, как корень ирр. эл-та, с помощью к-рого прошло расширен, имеет корнем исходного полинома:

$x^2+5x+3=0 \Rightarrow x^2 = -5x-3 \Rightarrow x^2 = 2x+4$
$-5 \bmod 7 = 2;\quad -3 \bmod 7$

т.о. 2-й эл-т $2x+4$

$x^3 = 2x^2+4x = 2(2x+4)+4x = 4x+1+4x = x+1$

3-й эл-т $x+1$

3-й ряд $x^4 = x^2 + x = 2x + 4 + x = 3x + 4$

4-й ряд $x^5 = 3x^2 + 4x = 3(2x+4) + 4x =$
$= 6x + 12 + 4x = 3x + 5$

6-й ряд $x^6 = 3x^2 + 5x = 3(2x+4) + 5x =$
$= 11x + 8 = 4x + 5$

7-й ряд $x^7 = 4x^2 + 5x = 4(2x+4) + 5x =$
$= 13x + 16 = 6x + 2$

8-й ряд $x^8 = 6x + 2x = 12x + 24 + 2x = 3$

9-й ряд $3x$

10-й ряд $6x + 5$

11-й ряд $3x + 3$

12-й ряд $2x + 5$

13-й ряд $2x + 1$

14-й ряд $5x + 1$

15-й ряд $4x + 6$

16-й ряд 2

17-й ряд $2x$

18-й ряд $4x + 1$

19-й ряд $2x + 2$

20-й ряд $6x + 1$

21-й ряд $6x + 3$

22-й ряд $x + 3$

23-й ряд $5x + 4$

24-й ряд 6

⋮

18 1.

Чтобы получилось поле, нужно ребавить "0"

Описание фактор группы.

Пусть G – группа и существует правильное разбиение группы по нормальному делителю H. Тогда смежные классы вместе с норм. делителем образуют группу.

Здесь H играет роль единицы, т.к.

$$aHH = aH^2 = aH$$

Определим умножение двух смежных классов: aH, bH:

$$aHbH = abH^2 = abH$$

Т.к. a и b принадл. разным смежным классам, то и ab определ. новый смежный класс.

Для aH определим обратн. эл-т в виде $a^{-1}H$.

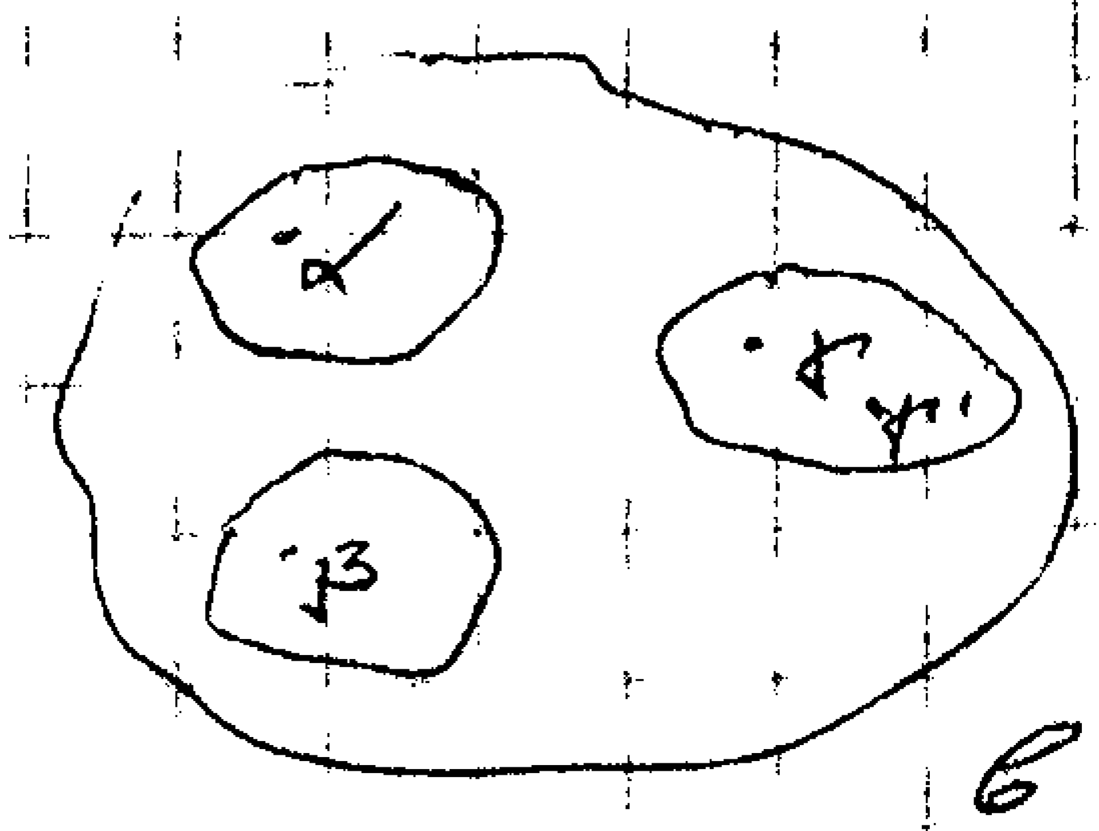
$$aHa^{-1}H = H^2 = H.$$

Т.о. определили групповую операцию на смежных классах. Но эл-тами группы являются смежные классы и характ. их составом смежного класса слишком громоздко.

Ранее установлено, что произвольный эл-т в смежном классе полностью х-зует этот класс.

Выберем произв. образом из каждого смежного класса по одному эл-ту.

Выбранные эл-ты в общем случае группу не образуют.



Применим групповую операцию к эл-там α и β. Пусть результат операции находится в множестве с γ, но он в общем случае не равен γ. Поэтому часто данное соотнош. запис. в виде

$$\alpha\beta = \gamma\, m_{\alpha\beta}$$

$m_{\alpha\beta}$ – m-фактор.

След-но m-факторы нужно вычислять от всевозможных произведений.

Описание получилось громоздкое. каждую с α, β и γ необх для каждой пары определить m-фактор. Поэтому в большинстве случаев изучают структуру группы и представители выбирают с учетом того, чтобы они образовали группу

Основы теории пространств.

1. Линейное векторное пространство.

Пусть M - множество с элементами произвольной природы. Назовем их векторами. Определим на эл-тах операцию сложения. Пусть по сложению вектора образуют Абелеву группу. Определим на множестве умножение на число, принадлежащее заданному полю (о-р-е подразумевает нахожд результата операции в данном же множестве) Определим эл-т, играющий роль единицы. Пусть выполняются соотношения:

$$\alpha(x+y) = \alpha x + \alpha y$$
$$\alpha \beta x = \alpha(\beta x)$$
$$(\alpha+\beta)x = \alpha x + \beta x,$$

где α, β - числа;
x, y - векторы

Полученное множества называется векторным пространством

В векторном пр-ве обязат-но опр-ют базис, как максимальное число линейно независ. векторов с помощью которых можно выразить любой вектор пр-ва

Подпространство.

Выделим в рассм. множестве подмножество, для которого выпол. все условия векторного пр-ва. Тогда оно называется подпр-вом.

Ортогональное дополнение.

Рассм некое подпр-во вект пр-ва. Определим в нем скалярное пр-ние для двух векторов
Выберем вектор вне подпр-ва, который орто-гонален каждому вектору подпр-ва. Т.е вектор ортогонален подпр-ву.
Найдем все векторы, ортогон подпр-ву. Они образуют подмножество, назыв. ортогон дополнение к подпр-ву. В большинстве случаев рассм вект пр-ва, которое разлагаются на подпр-ва и ортогон. дополнения к нему

2. Афинные пространства.

Рассм векторные пр-ва, элементами которого являются векторы. Дополним их новыми объектами - точками, так, что для каждого вектора опр-ся начальная и конечная т-ки, при этом выполняются следующие условия,
- для каждой т-ки и произвольного вектора, для котор. данная т-ка начальная, всегда можно опред. еще т-ку, назыв. конечной.
- для 3 т-чек M, N, P всегда найдутся 3 вектора $\vec{MN}$, $\vec{NP}$, $\vec{MP}$ таких, что

$$\vec{MN} + \vec{NP} = \vec{MP}$$

Такое пр-во - афинное.

Выделим в пр-ве т-ку, которую назовем начальной. Тогда любую др. т-ку можно опр-ть, совместив начало соотв. вектора с начальной т-кой
Пусть в вект. пр-ве имеется базис. Разложив данный вектор в этом базисе, получим набор координат, которые назовем коорд. т-ки.
Т.е в афинном пр-ве т-ка опр-ся как набор чисел.

Плоскости

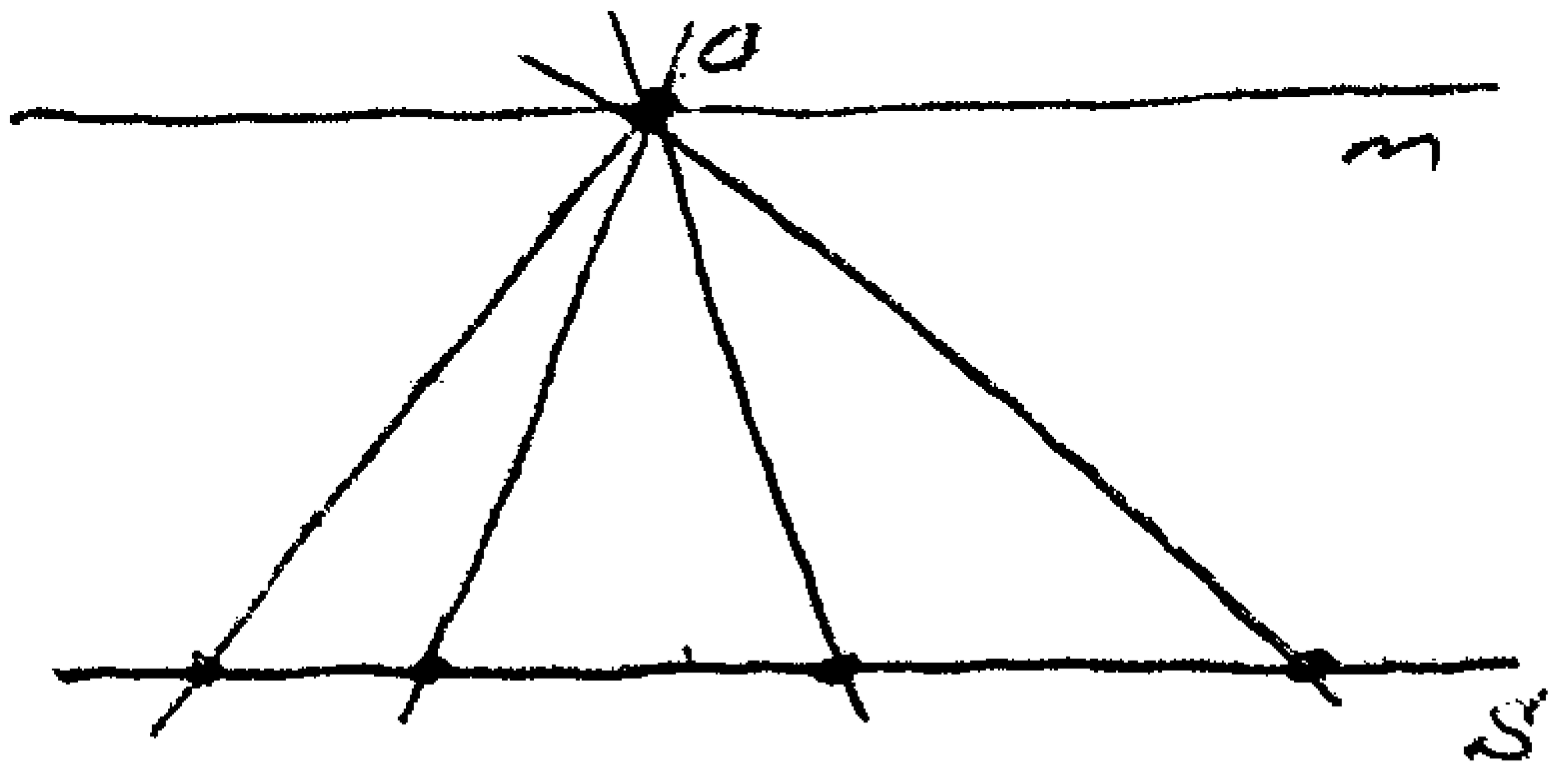
Рассм. в аффинном пр-ве совместную систему ур-й:

$$a_{11}x_1 + a_{12}x_2 +.. + a_{1n}x_n = b_1;$$
$$a_{21}x_1 + a_{22}x_2 +.. + a_{2n}x_n = b_2;$$
$$\cdots$$
$$a_{m1}x_1 + a_{m2}x_2 +.. + a_{mn}x_n = b_m$$

Пусть ранг матрицы левой ч-ти системы равен r. Тогда множество точек аффинного пр-ва, удовл. данной системе опр-ет k-мерную пл-ть, причем $k = n - r$.
Если пл-ть имеет размерность $(n-1)$, то она наз-в. гиперпл-ю.

3. Проективное пространство

Возьмем двумерную пл-ть, которую обозначим R^2, т.е. две коорд. в этой пл-ти - действит. числа. Возьмем прямую S и т-ку a вне её. Проведем через a семейство прямых, пересекающих S.



Тогда каждой т-ке пересеч. будет соотв. прямая. Но прямой, параллельной S не соотв. ни одна т-ка. Определим бесконечно удален. т-ку как т-ку пересеч. прямой, проход. через a, парал-ную S.

Все множество прямых, парал. m, пересекаются с S в одной т-ке. Т.е. получаем класс парал. прямых, пересек. в одной бесконечно удаленной т-ке.

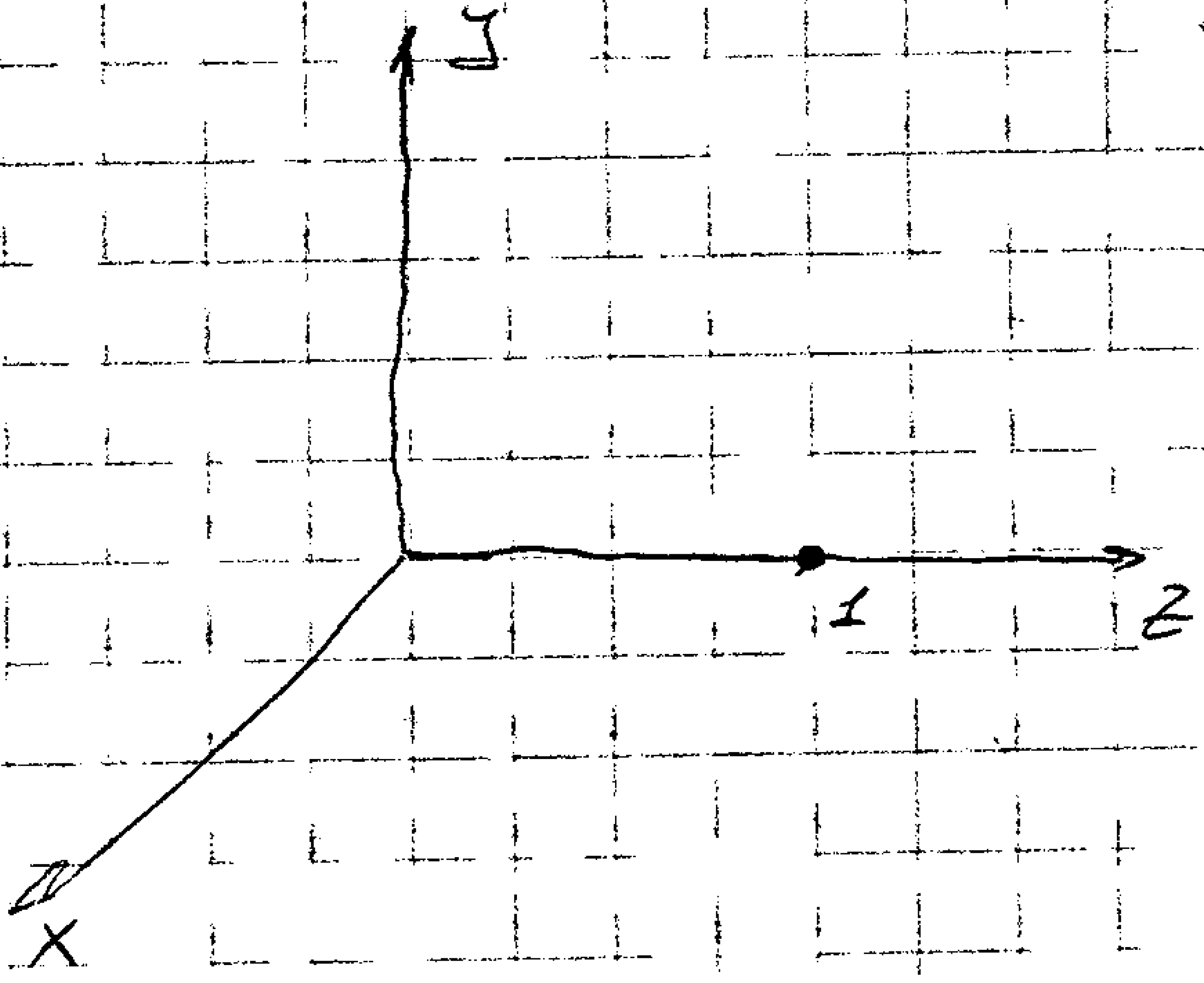
Возьмем другую S. Тогда опред. новое семейство парал. прямых и определим новую бесконечно удаленную т-ку

Т.о. вся пл-ть R^2 разбивается на классы эквивалентности – семейство парал-ных прямых

Множество всех бесконечно удаленных точек образуют бесконечно удаленную прямую. Т.е. дополнив пл-ть бесконечно удаленной прямой получаем проективную плоскость.

Возникает „неравенство" между „обычными" т-ками, которые могут быть определены через координаты, и бесконечно удаленной т-кой, котор опр-ся как пересечение парал. прямых.

Для того, чтобы выражать все т-ки схожим образом введем систему однородных координат. Для этого рассм 3-х мерное пр-во R^3.



Проведем через т-ку $z = 1$ пл-ть $z = 1$.

Пусть вложенная пл-ть будет исходной пл-ю R^2

Проведем через начало коорд. семейство прямых, пересекающих пл-ть $z = 1$.

Тогда каждая прямая опред. некотор. т-ку на пл-ти.

Каноничн. ур-е прямой $\frac{x}{p_1} = \frac{y}{p_2} = \frac{z}{p_3}$

p_1, p_2, p_3 – направляющие к-ты прямой.

Умножим p_1, p_2, p_3 на к-т $\lambda \neq 0$. Тогда ур-е прямой не изменится т.е p_1, p_2, p_3 можно взять за координаты, х-зующие т-ку на пл-ти $z = 1$ причем определены они неоднозначно, т.е.

$$(p_1, p_2, p_3) \sim (\lambda p_1, \lambda p_2, \lambda p_3).$$

Поэтому данные коорд опред не столько их значением, сколько их отношением, поэтому они запис. как: $p_1 : p_2 : p_3$.

Тройка $\left(\frac{p_1}{p_3} : \frac{p_2}{p_3} : 1\right)$ будет соотв т-ке непосредств на пл-ти $z = 1$.

Данные координаты (тройки чисел) называются однородными
Чтобы определить бесконечно удален. т-ку нужно положить $P_3 = 0$, т.е $(P_1; P_2 : 0)$.

Часто опр-е проективн. п-ти дается как множество прямых, проход. через начало коорд в трехмерном пр-ве. Данное опр-е расспр-ют на пр-во большей размерности. Пусть имеется пр-во с коорд $X_1, X_2, .., X_n$. Чтобы сделать его проективным, его вкладывают в пр-во на единицу большей размерности. При этом часто дополнит. коорд. обознач. X_0 и помещают на первое место:

$$(X_1, X_2, .., X_n) \mapsto (1, X_1, X_2, .., X_n).$$

Основные свойства конечных полей.

В большинстве случаев рассм. расширение простых полей, т.е. полей, которые не имеют нетривиальных подполей, а след-но, не получаются расширением. В этом случае кол-во эл-тов в расшир поле будет p^m. где p – х-ка поля (простое число), m – степень расширения. Совпадает с размерностью используемого полинома.

Для практич. приложений в основном использ. поля с $p = 2$. Поле можно рассм. как векторное пр-во, т.к. его элементами являются полиномы, которые можно представить как вектор след-но в поле вводим базис $\Theta_1, \Theta_2, .., \Theta_m$. Основным базисом является каноническим
Канонич. базис сост из векторов (полиномов), весь имеющ. один отличный от нуля элемент.

Существ и др базисы, по которым можно разложить вектор.

Поле обозначают: $GF(p^n) = F_{p^n} = F_q$ $q = p^n$.

Данное поле - поле разложения (на множестве многочленов) многочлена $X^{p^t} + X = X(X^{p^t-1} + 1)$.

$p^t + 1$ - порядок мультипликативной группы поля.

Разложение многочлена состоит из p^n - тов $(x - \alpha^i)$, где α - образующ. эл-т мультипликативной группы поля, i - принимает все возможные значения, т. е. все эл-ты поля являются корнями данного ур-я.

Кроме данного многочлена существ. многочлены и меньшей степени, у которого корни - эл-ты поля. Данный многочлен можно разложить на пр-ые многочлены, к-ты которого будут принадлежать полю F_p.

Рассмотрение многочленов минимальной степени, для которого данный эл-т поля является корнем называется минимальным многочленом для данного эл-та.

Циклотомические классы.

Пусть $p = 2$ Имеем поле $GF(2^m)$. Очевидно, что кол-во эл-тов в мультипликативной группе будет равно $2^m - 1$.

Рассм все числа от 1 до $(2^m - 2)$ по модулю $2^m - 1$.

Возьмем эл-т из этого ряда s.

Составим последовательность:

$$s, s2, s2^2, \ldots, s2^{n_s - 1}$$

Данная послед-ть образует цикл:

$$s2^{n_s} = s \bmod (2^m - 1).$$

Данный ряд - циклотомический. Каждому эл-т

этого ряда отличается от другого. Все э-ты ряда образуют циклотомич ряд для данного S. Возьмем следующее S, не принадлежащее данному ряду. Получим новый циклотомич класс Т.о. Все множество расм чисел разбивается на непересекающ. циклотомич. классы

n_s делит m без остатка

n_s - длина циклотомич. класса.

Рассмотрим э-ты, принадлеж. каждому циклотомич классу как индексы i.

Возьмем первый класс и расчитаем для индексов, входящих в него, α^i. Где α - образующ э-т поля. Тогда получим циклокласс.

Проделаем то же самое со всеми оставшимися классами и получим все множество циклоклассов. Все э-ты поля разбиваются на непересекающ. циклоклассы. ~~[illegible]~~ Причем длина циклокласса равна n_s.

След элементов

Пусть дано производное поле F_{q^m}.

Определим для э-та $a \in F_{q^m}$ отображение из поля ~~[illegible]~~ $F_{q^m} \to F_q$. Ф-ция создающая отображение называется ф-ция-след. Она обозначается

$$Tr_{F_{q^m}/F_q}(a).$$

Если q - простое, то ~~ф~~ ф-ция обозначается ~~как~~ $Tr_m(a)$.

$$Tr_{F_{q^m}/F_q}(a) = a + a^q + a^{q^2} + . + a^{q^{m-1}}$$

Автоморфизм Фробениуса.

Автоморфизмом называется отображение поля в себя. При этом эл-ты основного поля остаются неподвижными. Наиб. распр-е получил автоморфизм Фробениуса

$$\sigma_d(a) = a^{q^d}$$

при $q=2$ $\quad \sigma_d(a) = a^{2^d}$

Если данный автоморфизм применить к эл-ту, то след нового эл-та не изменится.

Описание булевых ф-ций через ф-цию-след

Рассм. множество полиномов K с нулевым свободным членом, степень которых не превосходит 2^n-2.
Рассм. любой базис в данном поле: $\theta_1, \theta_2, \dots, \theta_n$.
Произвольный эл-т запишем в виде:

$$X = x_1\theta_1 + x_2\theta_2 + \dots + x_n\theta_n,$$

где $x_1, x_2, \dots, x_n$ - булевы переменные $\{0, 1\}$

Рассм. полином $P(X) \in K$, в котором X задается коорд. $(x_1, x_2, \dots, x_n)$. Вычислим ф-цию-след:

$$Tr_n P(X) = Tr_n \left[\sum_{i=1}^{2^n-2} a_i X^i \right] \qquad a_i \in F_{2^n}.$$

Задаем всевозможные наборы $(x_1, x_2, \dots, x_n)$.
Тогда получаем значение, которое опр-ет какую-то булеву ф-цию.
Обозначим эту булеву ф-цию как $f_P(x_1, x_2, \dots, x_n)$.

Разные полиномы $P(X)$ могут давать одинак. значения следов при всех наборах $(x_1, x_2, \dots, x_n)$.
Такие полиномы - эквивалентные по следу. Иначе - не эквивалентные по следу

Кроме этого при $x=0$ все булевы ф-ции принимают значение 0.

Т 0. полиномов недостаточно для описания всех булевых ф-ций.

Рассм. для данного поля разбиение на циклотомические классы. Возьмем в каждом циклотомическом классе по представителю (минимальное число классов) и объединим их в множество, которое обозначим Π_n.

Рассм. полином $\sum_{s \in \Pi_n} a_s x^s$ - называется циклотомическим представителем полинома.

Каждый полином из множества K называется неприводимым циклотомическим представителем полиномом.

Семинар

---

x^2+x+2. Построить поле Галуа 5^2.

1. Для $GF(5)$

Вычеты по модулю 5: $0, 1, 2, 3, 4$

Приведен. полином вида $x^2+x+2=0$

$x^2+x = -2-x$ - Записываем обратно

$x^2 = 3+4x$

Строим циклотомические группы.

1 x

2 $x^1 = 4x+3$

3 $x^3 = 4x^2+3x = 4(4x+3)+3x = 19x+12 = 4x+2$

4 $x^2(4x+2) = 4x^2+2x = 4(4x+3)+2x = 18x+12 = 3x+2$

5. $(3x+2)x = 3x^2+2x = 3(4x+3)+2x = 14x+9 = 4x+4$

6. $(4x+4)x = 4x^2+4x = 4(4x+3)+4x = 20x+12 = 2$

7. x^7

8. $x^8 = x^2(4x+3) = 8x+6 = 3x+1$

9. $(3x+1)x = 3x^2+x = 3(4x+3)+x = 13x+9 = 3x+4$

10. $(3x+4)x = 3x^2+4x = 3(4x+3)+4x = 16x+9 = x+4$

11. $(x+4)x = x^2+4x = 4x+3+4x = 8x+3 = 3x+3$

12. $(3x+3)x = 3x^2+3x = 3(4x+3)+3x = 15x+9 = 4$

13. $4x$

14. $4x^2 = 4(4x+3) = 16x+12 = x+2$

15. $(x+2)x = x^2+2x = 4x+3+2x = 6x+3 = x+3$

16 $(x+3)x = x^2+3x = 4x+3+3x = 7x+3 = 2x+3$

17. $(2x+3)x = 2x^2+3x = 2(4x+3)+3x = 11x+6 = x+1$

18 $(x+1)x = x^2+x = 4x+3+x = 5x+3 = 3$

19 $3x$

20 $3x^2 = 3(4x+3) = 12x+9 = 2x+4$

21. $(2x+4)x = 2x^2+4x = 2(4x+3)+4x = 12x+6 = 2x+1$

22. $(2x+1)x = 2x^2+x = 2(4x+3)+x = 9x+6 = 4x+1$

23. $(4x+1)x = 4x^2+x = 4(4x+3)+x = 17x+12 = 2x+2$

24 $(2x+2)x = 2x^2+2x = 2(4x+3)+2x = 10x+6 = 1$

↑ степень
x (логарифм)

Чтобы построить поле, нужно добавить нулевой элемент. Часто эл-ты нумеруют модифицир логарифмами, котор отлич. от обычного добавл единицы. При этом единич эл-т ставят первым, а далее идет мультипликативная группа.

Обычно таблица умножения и сложения составл. не для полиномов, а для модифицир логарифмов.

Нахождение полинома, эквивалентного по следу

Пусть $P(x) \in K$, т.е.

$$P(x) = \sum_{i=1}^{2^n-2} a_i x^i$$

$$P(x) = \sum_{s \in \Gamma_s} a_s x^s$$

Запишем индекс i через представителя S и номер индекса в циклотомич. классе j:

$$i = S 2^j$$

Тогда:

$$P(X) = \sum_{s \in n} \sum_{i=0}^{n_s - 1} a_{s \cdot 2^i} X^{s \cdot 2^i} = \sum_{s \in n} P_s(X)$$

$P_s(X)$ – циклотомический приведенный полином

$$P_s(X) = \sum_{i=0}^{n_s - 1} a_{s 2^i} X^{s 2^i}.$$

Применим к n-ому полиному P_s автоморфизм Фробениуса. Тогда его след не изменится тогда след полинома P_s вычислим:

$$Tr_n(a_{s 2^i} X^{s 2^i}) = Tr_n(a_{s \cdot 2^i}^{2^t} X^{s \cdot 2^{i+t}}),$$

t – выбирается произвольно.

Выберем $t = n_s - i$, тогда получим след:

$$Tr_n(a_{s \cdot 2^i}^{2^{n_s - i}} X^s).$$

Рассмотрим цепочку равенств для $P_s(X)$:

$$Tr_n[P_s(X)] = Tr_n \sum_{i=0}^{n_s - 1} Tr_n(a_{s \cdot 2^i} X^{s \cdot 2^i}) =$$

$$= \sum_{i=0}^{n_s - 1} Tr_n(a_{s 2^i}^{2^{n_s - i}} X^s) = Tr_n\left[X^s \sum_{i=0}^{n_s - 1} a_{s 2^i}^{2^{n_s - i}}\right]$$

Циклотомически приведенный полином при задании s зависит по следу только последнего выражения с X^s.

След-но, произвольный полином $P(X)$ будет зависеть по следу суммы всевозможных полиномов при всех s из множества представителей

Т о, выписав все возможные полиному. через по следу, построим новый полином:

$$P'(X) = C_0 \alpha + P(X) + C_{2^n - 1} \alpha X^{2^n - 1}$$

$C_0, C_{2^n-1} \in \{0, 1\}$
α - эл-т поля, со следом, равным 1.
Полиномов $P'(x)$ достаточно для описания любых булевых ф-ций

Основные понятия теории кодирования

Рассм. общий случай: A - множество эл-тов, называемых алфавит.
$q = |A|$ - мощность алфавита.
Сформируем объект - декартово произведение вида:

$$\overbrace{A \times A \times A \times .. \times A}^{n} = A^n$$

Эл-тами получ. множества являются кортежи из n эл-тов.
Возьмем $C \in A^n$ - подмножество A^n.
$|C|_{ER}$ - мощность C
Вводится логарифмич. мощность $k = \log_q |C| \in R$.
В практич. применениях рассм-ся k из натурального ряда.
Подмножество C называется кодом с параметрами $[n, k, d]_q$.
n - длина кода (кортежа); каждая позиция в кортеже называется координатой, а элемент кода называется кодом слова.
k - длина информационного слова.
В произв. множествах неопределена метрика, поэтому в кач-ве простейшей выбирают метрику Хемминга.
Возьмем произв. пару слов. Рассм соотв координаты в двух словах и посчитаем кол-во несовпадающих координат. Это Хемминговое расстояние между словами.

Рассм. все возможные пары и найдем минимальное значение Хеммингово расстояния. Оно называется минимальным кодовым расстоянием d.

Линейные коды

Пусть поле F_q, где $q = p^k$.
Расм. аффинное пр-во F_q^n. Выделим в данном пр-ве линейное подпр-во C. Размерность этого пр-ва обозначим k. ~~Следов.~~ Тогда C - код в пр-ве F_q^n.

Пусть имеется поток символов передаваемой информации. Разделим его на блоки длиной k символов. Отобразим подпр-во F_q^k на подпр-во F_q^n, т.е. каждому информац. слову, длиной k символов поставим в соотв-ие кодовое слово, длиной n символов. Получилось слово большей длины. $(n-k)$ - избыточность кода.

При прохождении канала получ. кодовое слово претерпевает искажения. После извлечения из канала необх. определить, какое слово передавалось. Обычно расм. метод максимального правдоподобия, в соотв с которым ищется ближайшее кодовое слово к принятому. Но этот метод сложен и имеет ограничения.

Расм. пр-во F_q^n и выделим в нем отдельные точки, соот-щие кодовым словам, входящим в подпр-во C. Расм две соседние т-ки. Расст между ними не превышает d.
Принадлежность принятого слова к какому-либо кодовому может быть однозначно определено, если оно находится на расст. не более $\frac{d-1}{2}$.

Расм-ная максимальная удаленность от кодового слова х-ся расст до него, а, след-но, и кол-во ошибок.
Окружим каждое кодовое слово сферой, радиусом $t = \left[\frac{d-1}{2}\right]$ - максимально допустимое кол-во ошибок.
Обычно проводится анализ канала и опред. величина t. После этого строится код для обнаружения t ошибок

Порождающая матрица.

Преобразование $F_q^k \to F_q^n$ реализуется в матричном виде. Для этого в кодовом пространстве выделим k линейно независимых векторов с координатами $C_1^{(1)}, C_2^{(1)}, \dots, C_n^{(1)}$

$C_1^{(2)}, C_2^{(2)}, \dots, C_n^{(2)}$

$\dots\dots\dots\dots$

$C_1^{(k)}, C_2^{(k)}, \dots, C_n^{(k)}$

Составим матрицу из этих векторов, выбирая в качестве строк координаты указанных векторов:

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

Пусть информационное слово из k символов - A, тогда кодовое слово $C = A \cdot G$

Дуальные коды.

Рассм в F_q^n подпр-во, являющееся ортогональным дополнением подпр-ву C. Это подпр-во состоит из векторов длины n, а размерность подпр-ва $(n-k)$. Каждый вектор подпр-ва ортогонален вектору из C. Сформируем код с параметрами: $[n, n-k, d_1]_q$.

Очевидно, что длина информационного слова $(n-k)$, d_1 в общем виде определить сложно. Пусть отображение $(n-k)$ символов в n символов данного подпр-ва. Для этого составим матрицу H. Код называется дуальным коду C с порождающей матрицей H с размерностью $(n-k) \times n$

Возьмем произв. кодовое слово из C. Умножим C на H^T. Получим нулевой вектор, т.к. любое кодовое слово ортогонально исходному кодовому слову.

Т.е. $GH^T = 0$.

, чтобы безусловный вектор из G отличался любому безусловному вектору из H. След-но, $eH^T = 0$. Но кодовые слова - линейные комбинации безусловных векторов порождающей матрицы. След-но, произведение вектора из C будет отлично любому безусловному вектору в H и $cH^T = 0$.

Тогда H можно использ. как проверочную матрицу, т.е. условие любой вектор из C на H^T, говорит, что $c \in C$, если при перемножении получаем нуль-вектор.

Соотношение Синглтона

Весовая особенность

В линейных кодах кол-во ненулевых компонент кодового слова назыв его весом. Вес линейного кода равен миним. кодов. расст. равно минимальному весу кодового слова.

Возьмем кодовое слово с с миним. весом d. Т.к. $cH^T = 0$, то матрица H должна быть d линейно зависимых столбцов и (d-1) линейно независимых.

Ранг матрицы H (n-k)

Очевидно, что должно выполняться соотношение

$(n-k) \geq d-1$.

Тогда:

$d \leq n-k+1$ - соотношение Синглтона

Это неравенство является границей, но используется для качественной оценки параметра.

Матрица Вандермонда.

Часто встречающаяся и довольно удобная для вычислений в специальном виде матрица имеет вид:

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{bmatrix}$$ — Матрица Вандермонда

$x_1, x_2, \dots, x_n$ — разные числа

Основное св-во данной матрицы в том, что ее определитель:

$$\Delta = \prod_{1 \le i < j \le n} (x_j - x_i)$$

Вычтем первый столбец из всех остальных:

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ x & x_2 - x_1 & x_3 - x_1 & & x_n - x_1 \\ x_1^2 & x_2^2 - x_1^2 & x_3^2 - x_1^2 & & x_n^2 - x_1^2 \\ \dots & \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} - x_1^{n-1} & x_3^{n-1} - x_1^{n-1} & \dots & x_n^{n-1} - x_1^{n-1} \end{bmatrix}$$

Разложим данный опр. по первой строке

$$\begin{vmatrix} x_2 - x_1 & x_3 - x_1 & \dots & x_n - x_1 \\ x_2^2 - x_1^2 & x_3^2 - x_1^2 & \dots & x_n^{n-1} - x_1^{n-1} \\ \dots & \dots & \dots & \dots \\ x_2^{n-1} - x_1^{n-1} & x_3^{n-1} - x_1^{n-1} & \dots & x_n^{n-1} - x_n^{n-1} \end{vmatrix}$$

прибавим к каждой строке предыдущую, умноженную на x_1.

$$\begin{vmatrix} x_2-x_1 & x_3-x_1 & \dots & x_n-x_1 \\ x_2(x_2-x_1) & x_3(x_3-x_1) & \dots & x_n(x_n-x_1) \\ \dots & \dots & \dots & \dots \\ x_2^{n-2}(x_2-x_1) & x_3^{n-2}(x_3-x_1) & \dots & x_n^{n-2}(x_n-x_1) \end{vmatrix}$$

Вынеся из каждого столбца общие множители:

$$\Delta = (x_2-x_1)(x_3-x_1)\dots(x_n-x_1)\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_2 & x_3 & \dots & x_n \\ x_2^2 & x_3^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_2^{n-2} & x_3^{n-2} & \dots & x_n^{n-2} \end{vmatrix}$$

Поступая аналогично с новым определителем, вынося за скобки новые множители и получим, что определитель есть n-ое множество множителей. Он отличен от нуля, если все x_i различны.

Такие и определитель Вандермонда приводится определителю вида:

$$\Delta_1 = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots \\ x_1^{p-1} & x_2^{p-1} & \dots & x_n^{p-1} \\ x_1^{p+1} & x_2^{p+1} & \dots & x_n^{p+1} \\ \dots & \dots & \dots & \dots \\ x_1^n & x_2^n & \dots & x_n^n \end{vmatrix}$$

Здесь степень p "пропущена".

Для установления значения определителя расм. столбец определителя.

Расм. $x_1, x_2, \dots, x_n$ и их степени $1, 2, \dots, n$. Дополним определитель новым столбцом:

$$\begin{vmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ x & x_1 & x_2 & x_3 & \dots & x_n \\ x^2 & x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ x^n & x_1^n & x_2^n & x_3^n & \dots & x_n^n \end{vmatrix}$$, где x – переменная.

Вычисление данного определителя приводит к получению полинома от x, вида:

$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$,

a_i - постоянные к-ты.

По другому данный опр-ль можно вычислить, разложив его по первому столбцу. При этом к-ты при степенях x получаем определители рассматриваемого вида Δ_1.

Рассм. к-т a_0. Очевидно, что $a_0 = \Delta$.

$x_1, x_2, \ldots, x_n$ - корни полинома $f(x)$

Для вычисления к-тов a_i воспользуемся теоремой Виета

$$x_1 + x_2 + \ldots + x_n = -\frac{a_1}{a_0}$$
$$x_1x_2 + x_2x_3 + \ldots + x_{n-1}x_n = \frac{a_2}{a_0}$$
$$x_1x_2x_3 + x_2x_3x_4 + \ldots + x_{n-2}x_{n-1}x_n = -\frac{a_3}{a_0}$$
$$\ldots$$
$$x_1x_2\ldots x_{n-1} + x_1x_2\ldots x_{n-2}x_n + \ldots + x_2x_3\ldots x_n = (-1)^{n-1}\frac{a_{n-1}}{a_0}$$
$$x_1x_2\ldots x_n = (-1)^n\frac{a_n}{a_0}$$

Получены все к-ты a_i, след-но, любой опр-ль вида Δ_1 может быть выражен через них.
~~Например~~ В дальнейшем рассматриваем пол Гоуа ~~...~~ размерностью 2^m. Для них отсутств. понятие знака „-".
Например:

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-2} & x_2^{n-2} & & x_n^{n-2} \\ x_1^{n} & x_2^{n} & & x_n^{n} \end{vmatrix} \quad p = n-1$$

Для вычисления данного определит. необходимо в дополнительном определителе использ. расширение по первому столбцу и предпоследней строке. ~~...~~ к-т при x^{n-1} имеет вид:

$$\Delta(X_1+X_2+\dots+X_n) = \Delta_1$$

Аналогично вычисляется любой определитель типа Δ_1.

$[n,k,d]_q$ системы.

Рассмотрим аффинное пространство размерности k. Расположим в нем т-ки, которые обозначим:
$\{P_1, P_2, \dots, P_n\} = \mathcal{P}$.
Множество точек $\mathcal{P}$ называется $[n,k,d]_q$ системой, если все они не лежат в одной гиперплоскости.

Параметры системы:

$n = |\mathcal{P}|$,
$k = \dim V$
$d = n - \max|H \cap \mathcal{P}|$

Под H подразумевается множество гиперпл-тей в пр-ве, из которой выбирается та гиперпл-ть, у которой максимальное кол-во т-к из множества $\mathcal{P}$.

Можно показать, что в любой $[n,k,d]_q$ системе можно поставить в соответствие линейный $[n,k,d]_q$ код.

Проективные $[n,k,d]_q$ системы.

Определим проективное пр-во $P = \mathcal{P}(V)$ (множество прямых)
Проективной $[n,k,d]_q$ системой называется множество точек (прямых) $\mathcal{P}$, которые целиком не лежат ни в одной проективной гиперплоскости.
Параметры системы:

$n = |\mathcal{P}|$
$k = \dim(\mathcal{P}+1)$
$d = n - \max(H \cap \mathcal{P})$

Любой проективный $[n, k, d]_q$ схеме можно поставить в соотв. $[n, k, d]_q$ код

Спектр кода

Рассмотрим линейный код. Очевидно веса кодовых слов будут распределяться от 0 до n. Всегда в линейном коде существ слово веса 0. Для линейных кодов сложение двух кодовых слов приводит к новому кодовому слову, т.е. должен присутствовать нулевой кодовый вектор.

Спектр записывают в виде,

$$W(X:y) = \sum_{r=0}^{n} A_r X^{n-r} y^r,$$

A_r - кол-во кодовых слов, имеющих вес r.
при $r = 0$, $A_0 = 1$.
Если $r < d$, то $A_r = 0$.
С учетом данного св-ва, формулу часто записывают в следующем виде:

$$W(X:y) = X^n + y^d \sum_{i=0}^{n-d} A_{d+i} y^i X^{n-d-i}$$

Семинар

Поле Галуа 2^4 имеет подполе, т.к. 4 делится на 2. Элементы этого подполя приводятся в материалах. Учитывая св-ва поля считаем, что аддитивная группа подполя является подгруппой адитивной группы всего поля. Адитивн. группа подполя является нормальн делит. в адитивн группе поля. Основн задачей являются нахож. смежных классов при разложении относит-но операции сложения. Для этого берем из вариантов первый элемент, котор. не принадлежит подполю и складываем его со всеми эл-тами подполя. Получаем смежный класс, соотв. первому эл-ту

~~Берем карту~~ В карте указаны модифицир. логарифмы элементов
Берем эл-ты подполя и наносим на эту карту.
Подполе нумеруется в модифицир. логарифмах, а поле - в логарифмах.

~~Берем смежный класс~~
Чтобы найти логарифмы эл-тов в смежном классе воспольз. второй таблицей поля, где нумерация идет по порядку.
По второй таблице находится логарифм эл-та смежного класса, прибавив 1, получаем модифицир логарифм. Др. цветом проставляем их на карте. Смежный класс не пересекается с нормальным делителем. То же самое повторяем для второго эл-та.

Берем два произв. эл-та в двух полученных классах. Считаем сумму этих эл-тов. Убедиться, что этот элемент не входит ни в один класс, ни в нормальный делитель

Берем этот эл-т и для него образуем третий смежный класс. Убедиться, что:
1) новый класс не пересек с другими;
2) сумма любых 2-х других эл-тов из 1-го и 2-го классов также лежит в третьем классе.

Эл-ты, имеющие нулевой след образуют подгруппу.

след 0) 0, 5, 13, 21, 29, 37, 45
1) 11, 20, 23, 33, 34, 38, 40
2) 1, 2, 6, 8, 27, 36, 39
3) 19, 28, 31, 41, 42, 46, 48.
4) 4, 7, 17, 18, 22, 24, 43
5) 3, 12, 15, 25, 26, 30, 32
6) 9, 10, 14, 16, 35, 44, 47.

Сложим нулевой и первый класс,
х-т23 и х-т5.

22: $X+3$
4: $3X+4$
$4X$ — 33 → 34, т.е нулевой класс выполняет роль нормального делителя.

Высшие веса кода (веса Вея).

Расм аффинное пр-во F_q^r. Выделим в нем подпр-во D размерности к. Очевидно, что $1 \leq k \leq r$. Рассмотрим все слова в подпр-ве D, которые содержат r координат. Подсчитаем кол-во коорд i, таких, что в подпр-ве D найдутся такие вектора x, что $x_i \neq 0$. Полученное значение наз-вается весом Вея к-го порядка d_k для данного подпр-ва

Расм. код в пр-ве F_q^r. В данном коде как в подпр-ве также расм. подпр-во меньшей размерности. Для заданной размерности подпр-ва таких подпр-в может быть несколько с различн. высшими весами. Зафиксируем миним. значение веса подпр-ва. Аналогично найдем все веса для всех размерностей подпр-в и получим высший весовой ряд, х-зующий код.
Очевидно, что $d_1 = d$.

Уравнение Мак-Вильямс.

Если задан весовой спектр кода $W_C(X:Y)$, то можно найти весовой спектр дуального кода $W_{C^\perp}(X:Y)$.

$$W_{C^\perp}(X:Y) = q^{-k} W_C[X+(q-1)Y : X-Y]$$

Иногда требуется отыскать не весь список двоичного кода, а только отдельные его компоненты. Связь между ними имеет вид.

$$A_i' = g^{-k} \sum_{j=0}^{n} A_j P_i(j)$$

A_i, A_j - спектральные компоненты двоичного и троичного кода,

$P_i(j)$ - числовая функция.

$$P_i(x) = \sum_{d=0}^{i} (-1)^d (g-1)^{i-d} \binom{x}{d} \binom{n-x}{i-d}$$

$\binom{x}{j} = \frac{x!}{j!(x-j)!}$ - число сочетаний из x по j.

Использование проверочных матриц.

Синдром.

Ранее установлено, что для кодового слова c:

$$cH^T = 0.$$

Пусть в канале в слово c внесены ошибки, которые x-ю вектором E. Он состоит из нулей и единиц ошибок

Напр. $E = (0,0,0,\dots, \underbrace{e_1,0,0,\dots, e_2,0,\dots, e_3,0,\dots,0}_{\text{ошибки}})$

Он x-ым позицию и величину ошибки получим искаженное слово V $V = c + E$.

Тогда используя проверочную матрицу:

$$VH^T = (c+E)H^T = \underbrace{cH^T}_{=0} + EH^T = EH^T = S$$

С помощью проверочной матрицы для искаженного слова можно вычислить вектор, который не зависит от слова, а зависит только от конфигурации вектора ошибок.
Данный вектор называется синдромом S.

По виду вектора S необх разработать алгоритм для нахожд номеров позиций ошибок и их величин.

Понятие циклических кодов.

Рассмотрим афинное пр-во F_q^n
Поставим в соответствие каждой n-ке набор её координат $c_0, c_1, \ldots, c_{n-1}$. Поставим в соот-е данному набору полином от одной перем x:

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} = C(x)$$

Степень полинома не превосходит $n-1$.

Набор координат также можно расм как кодовое слово. Сделаем циклический сдвиг:

$$c_{n-1}, c_0, c_1, \ldots, c_{n-2}$$

Если при этом получилось слово, принадлеж. тому же коду, что и предыдущ., то код – циклический

При описании с помощью полиномов сдвиг обычно опис умножением полинома на x.

Вычислим: $x \cdot C(x) = c_0 x + c_1 x^2 + c_2 x^3 + \ldots + c_{n-1} x^n$

Получившийся полином не может принадлежать коду, т.к. степень его превышает $(n-1)$.

Предположим, что $x^n = 1$, т.е. $x^n - 1 = 0$. Тогда

$x C(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2} x^{n-1}$ – слово, которое может принадлежать данному коду.

Введем другое описание данного эффекта. Для этого разделим $x\,C(x)$ на $x^n - 1$.

$$\frac{xC(x)}{x^n-1} = \frac{c_0x + c_1x^2 + \dots + c_{n-1}x^n + c_{n-1} - c_{n-1}}{x^n-1} =$$

$$= \underbrace{c_{n-1}}_{\text{целая часть}} + \underbrace{\frac{c_{n-1} + c_0x + c_1x^2 + \dots + c_{n-2}x^{n-1}}{x^n-1}}_{\text{остаток от деления}} = C_1(x)$$

Отсюда $C_1(x) = xC(x) \bmod (x^n-1)$.

При вычислениях по модулю (x^n-1) степени $xC(x)$ получим кодовые слова, образованные циклическими сдвигами от исходных.
Данная операция определена для всего линейного пр-ва F_q^n.
Выделим в пр-ве F_q^n подпр-во. Множество полиномов в F_q^n образуют кольцо полиномов. Учитывая, что аддитивная группа подпр-ва будет подгруппой аддитивной группы F_q^n можно сделать вывод, что данное подпр-во является подкольцом полиномов исходного кольца.

Данное подкольцо из полиномов из одной переменной является главным, т.е. получается пр-ием различных полиномов на некоторый полином $g(x)$, который является образующим полиномом данного подкольца.

Т.к. код - это подпр-во линейного пр-ва, то данное подкольцо полиномов будет кодом.

Потребуем, чтобы при умножении любого полинома из подкольца x результат принадлежал данному подкольцу. Данному условию удовлетворяет идеал кольца. След-но любой циклический код - это идеал в кольце полиномов с некоторым порождающим полиномом $g(x)$.

Порождающий полином имеет степень r.
Каждой информац. послед-ти (блоку) поставим
в соот-вие информац. полином $a(x)$. Кодовое
слово образуется как $a(x)g(x)$ причем расс-ся
информац. блоки такой длины, чтобы суммарная
степень не превышала $(n-1)$.

$$a(x)\,g(x) = C(x).$$

Допустим, что принято из канала слово $c(x)$.
Разделим его на $g(x)$. Если остаток равен нулю,
то данное слово - кодовое, если остаток ненулевой,
то он содержит в себе всю информацию об
ошибках, котор. слово приобрело в канале.
Данный остаток - синдром.

Коды Голея.

Возьмем в аффинном пр-ве т-ку, соот-щую
кодовому слову. Кол-во точек, наход. рядом с
ней, которые отличаются на одну коорд.
можно определить как $\binom{n}{1}$ (расм. двоичный код).
Соот-но, отличие в двух коорд. можно
расчитать как $\binom{n}{2}$ и т.д.
n - длина кодового слова.

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$$

левая часть - объем сферы, окружающ данное
кодовое слово, радиусом 3. След-но, если взять
кодовые слова длиной 23 символа, то весь код
может состоять из 2^{12} элементов. Если
каждый из них окружить сферой рад 3, то
код будет включать все т-ки под-пр-ва, отве-
денного ему.

Такой код должен иметь информац блок
длиной 12. Данный код должен определять
3 ошибки.

Как возмож. $t = \frac{d-1}{2}$, след-но данный код должен иметь миним кодовое расст. $d = 7$.
Т.е. код имеет параметры $[23, 12, 7]_2$

Для построения кода нужно определить порождающий полином $g(x)$. Если код является идеалом (подкольцом) и любое пр-ние полиномов в исходном кольце полиномов вычисляется по модулю $(x^n - 1)$, то порожд полином кода $g(x)$ должен делить без остатка полином $(x^n - 1)$.

Для нахождения $g(x)$ необходимо найти элемент порядка 23.
Найдем поле, в котором существует элемент порядка 23
Возьмем поле Галуа $GF(2^{11})$.

$(2^{11} - 1)$ - ~~мул~~ мощность мультипликатив группы поля.

$2^{11} - 1 = 89 \cdot 23$, след-но в поле 2^{11} существ элемент порядка 23. Пусть α - порожд элемент мультипликатив. группы 2^{11}. Тогда $\beta = \alpha^{89}$ - элемент порядка 23.
Если выбрано некоторое поле и длина кода совпадает с длиной мультипликатив группы, то такой код называют совершенным.
~~[illegible]~~
Для такого кода полином $(x^m - 1)$ разлагается на линейные множители, где m - длина мультипликативной группы.

Поступим аналогично: рассмотрим полином $(x^{23} - 1)$. Очевидно, что порождающий полином $g(x)$ должен делить данный полином без остатка. Построим двоичный код. Это значит, что полином $(x^{23} - 1)$ разложится на пр-ние минимальных полиномов в поле 2^{11}.

$$x^{23} - 1 = (x - 1)(x^{22} + x^{21} + \ldots + x + 1)$$

След-но второго способу нужно разложить на множители полином в данном поле.

Для этого найдем минимальные полиномы эл-ов β

Для минимальных полиномов можно легко будет

$\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^{32} = \beta^9, \beta^{18}, \beta^{36} = \beta^{13}, \beta^{26} = \beta^3, \beta^6, \beta^{12}, \beta^{24} = \beta$

$q(x) = (x+\beta)(x+\beta^2) \dots (x+\beta^{12})$

Построим поле Галуа α^{11}. Возьмем в этом поле образующий элемент α и найдем его 89 степень Все вычисления будем в модифицированных логарифмах.

Поле Галуа $GF(\beta^{11})$ строится с помощью полинома $x^{11} + x^6 + x^2 + x + 1$.

Выберем в кач-ве образующего эл-та α (примитивный логарифм).

Тогда $\alpha = 2$ $q_2(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$.

$\alpha = \alpha^{-1}$. $q_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$

Тогда:

$$x^{23} + 1 = (x+1) q_1(x) q_2(x)$$

Двоичные коды Голея

Такие, как и в случае двоичного кода Голея можно рассматривать поле Галуа $GF(3^5)$.

Видно, что:

$$\binom{11}{0} 2^0 + \binom{11}{1} 2 + \binom{11}{2} 2^2 = 243 = 3^5$$

Если код двоичный, то общее количество слов будет можно найти по ф-ле:

$$\binom{n}{i} (q-1)^i$$

i - кол-во расхождений с данным кодовым словом.

$q = 3$

Возникает вопрос, можно ли аналогичным способом построить код с параметрами $[11, 6, 5]_3$

$d = 2t+1 = 2\cdot 2+1 = 5$

Строим GF(3^5) с помощью полинома

$x^5+2x^3+2x^2+x+1$.

$(3^5-1) = 11 \cdot 22$ - в данном поле использ. $\beta=\alpha^{22}$

Ищем порождающий полином, разлагая полином (x^n-1) на многочлены, к-ты которых лежат в основном поле

Как и в предыдущем случае, потребуем, чтобы корни порождающего полинома было число β

Для опр-я др корней пороинд полинома определим циклотомич. классы по общей формуле. Также определяем циклоклассы. Т.о. получим, что корнями пороинд полинома будут $\alpha^1, \alpha^3, \alpha^4, \alpha^5, \alpha^9$.

Проводя аналогичные вычисления также можно получить 2 порождающих полинома:

$g_1(x) = x^5+x^4-x^3+x^2-1$

$g_2(x) = x^5-x^3+x^2-x-1$

Семинар

Таблица GF(2^3) x^3+x+1

Таблица сложения

0	1	2	3	4	5	6	7
1	0	4	7	2	6	5	3
2	4	0	5	1	3	7	6
3	7	5	0	6	2	4	1
4	2	1	6	0	7	3	5
5	6	3	2	7	0	1	4
6	5	7	4	3	1	0	2
7	3	6	1	5	4	2	0

Таблица умножения

0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	1
3	3	4	5	6	7	1	2
4	4	5	6	7	1	2	3
5	5	6	7	1	2	3	4
6	6	7	1	2	3	4	5
7	7	1	2	3	4	5	6

$(x+1)(x+2) = x^2 + x + 2x + 2 = x^2 + 4x + 2$

$(x+1)(x+2)(x+3) = x^3 + 4x^2 + 2x + 3x^2 + 6x + 4 = x^3 + 6x^2 + 8x + 4$

$(x^3+6x^2+3x+4)(x+4) = x^4 + 6x^3 + 7x^2 + 4x + 4x^3 + 2x^2 + 3x + 4 =$

$= x^4 + 3x^3 + 6x^2 + 6x + 1.$

$(x^4+3x^3+6x^2+6x+7)(x+5) = x^5 + 3x^4 + 6x^3 + 6x^2 + 7x + 5x^4 + 7x^3 + 3x^2 + 3x + 4 =$

$= x^5 + 2x^4 + 2x^3 + 4x^2 + x + 4$

$(x^5+2x^4+2x^3+4x^2+x+4)(x+6) = x^6 + 2x^5 + 2x^4 + 4x^3 + x^2 + 4x + 6x^5 + 7x^4 + 7x^3 + 2x^2 + 6x + 2 =$

$= x^6 + 7x^5 + 6x^4 + 5x^3 + 4x^2 + 3x + 2$

$(x^6+7x^5+6x^4+5x^3+4x^2+3x+2)(x+7) = x^7 + 7x^6 + 6x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 7x^6 + 6x^5 + 4x^4 + 3x^3 +$

$+ 2x^2 + x + 1 = x^7 + 1$

В $GF(2^3)$ полином (x^7+1) разлагается на

$x^7+1 = (x+1)(x+2)\cdot\ldots\cdot(x+7)$, причем все корни –

n-ого порядка.

$GF(2^4)$ образуется с помощью полинома x^4+x+1.

0. 0
1. 1
2. x
3. x^2
4. x^3
5. $x+1$
6. $(x+1)x = x^2 + x$
7. $(x^2+1)x = x^3 + x$
8. $(x^3+1)x = x^4 + x^3 + x^3 + x + 1$
9. $(x^3+x+1)x = x^4 + x^2 + x = x^2 + x + 1$
10. $(x^2+x+1)x = x^3 + x^2 + x$
11. $(x^3+x^2+x)x = x^4 + x^3 + x^2 = x^3 + x^2 + x + 1$
12. $(x^3+x^2+x+1)x = x^4 + x^3 + x^2 + x$
13. $(x^3+x^2+x)x = x^4 + x^3 + x^2 = x^3 + x^2 + x + 1$

14. $(x^3+x^2+x+1)\,x = x^4+x^3+x^2+x = x^3+x^2+1$

15. $(x^3+x^2+1)\,x = x^4+x^3+x = x^3+1$

16 $(x^3+1)\,x = x^4+x = 1$

Найдем все циклотомические классы в данном поле

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14

Циклотомические классы строятся

$S, S\cdot 2^1, S\cdot 2^2, \ldots, S\cdot 2^{n_s-1}$; $S\cdot 2^{n_s} = S \bmod 15$

S = 1 1, 2, 4, 8, (1)

S = 3 3, 6, 12, 9

S = 5 5, 10

S = 7 7, 14, 13, 11

Вычеркиваем индексы циклоклас-образующий эл-т "2" возводим её в степень эл-тов циклотом класса

S = 1 2, 3, 5, 9 $2^R = R+1$

S = 2 4, 7, 13, 10

S = 5 6, 11

S = 7 8, 15, 14, 12

эл-ты поля

$x^{15}+1 = (x+1)(x+2)\ldots(x+15)$.

2, 3, 5, 9

В поле $GF(2^4)$ взять 2-3 эл-та из ∀ получ. класса и вычислить их след

След $_{7^m}(a) = a + a^7 + a^{49} + a^{343}$

$q = 7,\ n = 4$

Рассм поле $GF(7^4)$ с полином $x^4+3x^3+5x^2+3x+5$.

Возьмем след эл-та $a = x^{611} = 6x^3+6$

$a^7 = x^{611\cdot 7} = x^{4277} = x^{1877}$

$a^{343} = x^{611\cdot 343} = x^{783}$

$a^{49} = x^{611\cdot 49} = x^{1139}$

$Tr_{7^m}(x^{611}) = \underbrace{6x^3+6} + \underbrace{x^3+5x^2+3x+5} + \underbrace{2x^3+6x^2+4x+2} +$

$+ \underbrace{5x^3+3x^2+3} = 3$

Декодирование кодов Голея

Для любых кодов возможны 2 способа декодирования:
- с помощью таблицы стандартного расположения кода;
- с помощью спец разработ алгоритма.

Для кодов Голея использ оба способа.

1. Метод таблицы стандартного расположения кода.

Выписываем в строку все кодовые слова. Первым словом в строке является нулевое кодовое слово. Рассм ситуацию, когда в канале могут быть ошибки, сначала одиночные. Можно выделить отдельн нулев столбец для ошибок или использовать столбец под нулевым кодовым словом.

Берем первую одиночн ошибку с единицей в младшем разряде. Прибавляем этот вектор к каждому кодовому слову, получаем 2-ю строку всевозможн ошибочных векторов с единичн ошибкой в первом разряде

	00000000000	00000102122	00000201211 ...	22020122121
00-…-01 →	00000000001	00000102120	00000201212 ...	22020122122
	00000000002	00000120121	00000201210 ...	22020122120
	00000000010	00000120102	00000201221 ...	22020122101
	20000000000	20000102122	20000201211	12020122121

Код (первая строка) является подгр-вом исходного аффинного пр-ва. След-но, можем рассм его как подгруппу в ~~—~~ группе всевозможных слов, точнее - нормальный делитель. Тогда каждая следующая строка - ~~—~~ смежный класс. Они не

пересекаются между собой. Закончив рассмотрение одиночных ошибок переходим к двойным ошибкам. И т.д., аналогично, к тройным

Найдем кол-во столбцов в таблице:

q^k столбцов

q – основание поля (у нас 3)
k – (у нас 6)
, т.е. 729 столбцов

Ранее сказано, что ошибки х-ся синдромом, который получается умножением принятого слова на проверочную матрицу.
Но синдром – вектор, длиной $(n-k)$, т.к. размеры матрицы H $(n-k) \times n$.

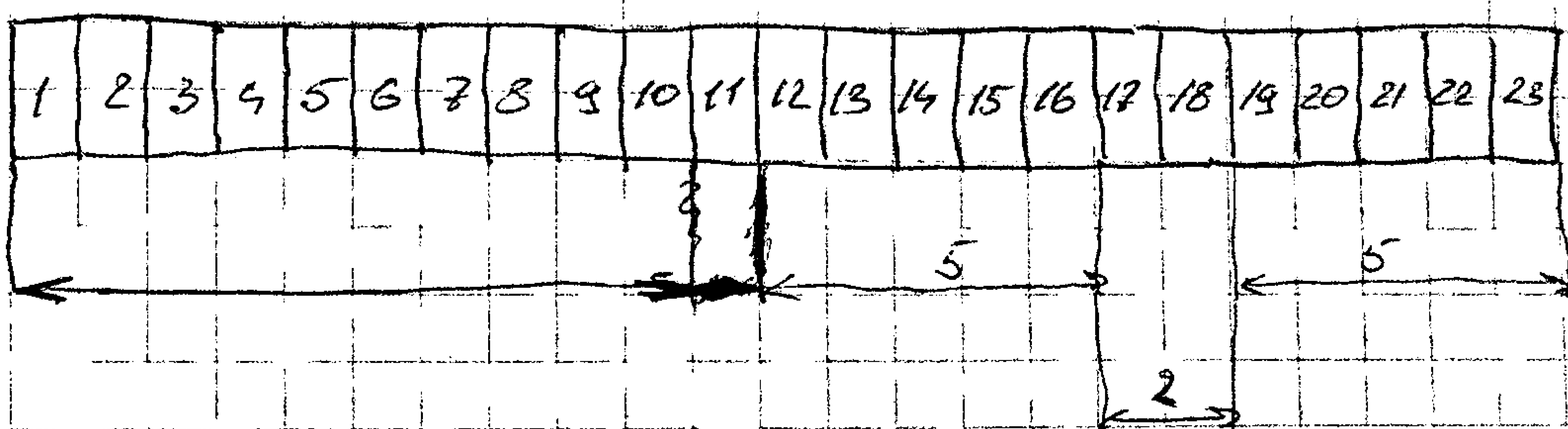
Очевидно, всего можно построить $q^{(n-k)}$ различных синдромов т.е. максимальное кол-во строк, которые можно строить $q^{(n-k)}$.

Для произвольного кода можем провести гориз. черту в некотором месте, которая ограничивает (сверху) анализир. входные векторы.

Допустим имеется вектор из канала. Найдем это слово в таблице стандартного расположения кода. Тогда определяем, что было передано слово, котор. стоит в начале столбца.
~~[illegible]~~ В первом столбце будут находится конфигурация ошибки в канале.

Для двоичного кода Голея был разработан специальный алгоритм декодирования, который называется методом ловли (вылавливания) ошибок. Рассм. несколько модифицированный алгоритм

Проанализир. структуру кодового слова кода [23, 12, 7]₂. Рассм. возможные варианты расположения ошибок в кодовом слове.
Синдром находим делением кодового слова на порожд. полином g(x).



Слева - младшие разряды принятого слова. Остаток от деления на g(x) имеет длину 11 разрядов. Выделим их на принятом слове.
Пусть все ошибки группируются в обл-ти этих 11 разрядов. Тогда конфигурация ошибок будет соотв. остатку от деления.

Т.к. код линейный, то можно рассматривать каждую ошибку в отдельности. Рассм. одиночн. ошибку, вход. внутри 11 разрядов. Записав полином, соотв. данной ошибке и разделив его на g(x) получим остаток от деления, равный исходному полиному.
Рассматривая аналогично др. искаженный бит в векторе конфигурации после суммирования можно получить различный остаток от деления, который соотв. вектору ошибки e(x).
Далее полученный вектор конфигурации ошибок прибавляем к младшим разрядам слова, при этом все ошибки компенсируются.

Признаком нахождения всех ошибок внутри 11 разрядов является величина веса остатка от

деления (синдрома). Если вес не превышает 3,
то предположение справедливо
Если ошибки были располож. компактно, но
никогда не в начале слова, то их можно привести
к началу путем послед-ного циклич. сдвига слова.

Существ. модификац., связанные с первичн. перестановкой координат, обнаружения вектора ошибок и обратной перестановкой.

Введем дополнительные признаки. Пусть имеет ошибочный бит, наход. вне расш. обл-ти, тогда остаток от деления приобретает больший вес. Возьмем одну или несколько позиций в слове и допустим, что в ней имеется ошибочный бит. Запишем для данного бита соотв. ему полином. Разделим данный полином на g(x). Получим величину остатка, соотв. ошибке именно в данном бите. Допустим, что два других ошибочных бита наход. внутри расш. обл-ти. Тогда, если к синдрому, получ. делением слова на g(x) прибавить остаток от деления для расш. бита, то останется синдром, соотв. конфигурации только 2-х ошибок в расш. обл-ти. Вес остатка не превышает 2.

Если ошибочн. бит вне обл-ти наход. в неизвестном месте, то его можно привести к известной позиции путем циклич. сдвига слова, предполагая, что остальн. ошибки не выходят за пределы расш. слова.

Для надежного определения трех ошибок в двоичн. коде Голея по данному алгоритму необх. определить, наличие каких ошибочных позиций проверяем.
Чтобы число циклич. сдвигов было минимальным при произв. конфиг. ошибок и данной симметрии кодового слова целесообразно

проверочный бит выбирают в середине остающейся части слова. Но в данном случае кол-во оставшихся бит - четные, поэтому в модифицир. методе ловли ошибок расслм. 2 проверочных бита.

Порядок декодирования двоичного кода Голея.

1 Найти синдром кодового слова т.е. найти остаток от деления слова на $g(x)$
2. Если вес получ. синдрома $W_1 \le 3$, то считаем, что синдром соотв. конфигурации вектора ошибок прибавляем его к слову (запись с младших разрядов) в этом случае декодир. закончено.
Если $W_1 > 3$, то идем далее
3 Прибавляем к синдрому остаток $x^{17} \bmod g(x)$. Если вес полученного синдрома ≤ 2, то прибавляем сумму к слову, т.е. исправляем 2 ошибки внутри расслм обл-ти
Для исправления 3-й ошибки нужно прибавить „1" к разряду x^{17}. Если вес > 2 идем далее
4. Прибавляем к синдрому $x^{16} \bmod g(x)$. Если вес синдрома $W_3 \le 2$, то прибавляем сумму к слову, и „1" к разряду x^{16}.
Если вес > 2 идем далее
5. Реализуем циклический сдвиг слова влево и повторяем алгоритм заново до исправления ошибок.
6. По окончании производим обратный циклический сдвиг
На каждом шаге необх. вычислять очередные значения синдрома. Анализир. левый разряд синдрома. Если он равен „1", то производится сдвиг синдрома на 1 разряд влево и сумму по mod 2 с $g(x)$, иначе реализуем только сдвиг влево, дополняя пустую позицию нулем

29 $(x^5+x+1)x = x+1$

20. $(x+1)x = x^2+x$

21 $(x^2+x)x = x^3+x^2$

22 $(x^3+x^2)x = x^5+x^3$

23 $(x^5+x^3)x = x^5+x^2+1$

24 $(x^5+x^2+1)x = x^3+x^2+x+1$

25. $(x^3+x^2+x+1)x = x^5+x^3+x^2+x$

26 $(x^5+x^3+x^2+x)x = x^5+x^3+1$

27 $(x^5+x^3+1)x = x^5+x^2+x+1$

28 $(x^5+x^2+x+1)x = x^3+x+1$

29 $(x^3+x+1)x = x^5+x^2+x$

30. $(x^5+x^2+x)x = x^3+1$

31 $(x^3+1)x = x^5+x$.

32 $(x^5+x)x = 1$

Метод бесповторного сложения в кодах Голея

Пусть $a(x)$ - информационное слово. Запишем его в виде полинома: $a(x) = x^{11}+x^8+x^7+x^5+x^3+1$.

Закодируем это слово с помощью $g(x)$.

$g(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$

$a(x)\cdot g(x) = (x^{11}+x^8+x^7+x^5+x^3+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1) =$

$= x^{22}+x^{21}+x^{18}+x^{16}+x^{15}+x^{14}+x^{13}+x^{21}+x^{18}+x^{17}+x^{16}+x^{15}+x^{13}+x^{10}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^3+x^{10}+x^9+x^6+x^5+x^3+x+x^{13}+x^{12}+x^{10}+x^8+x^7+x^5+x^3+1 =$

$= x^{22}+x^{21}+x^{19}+x^{16}+x^{14}+x^{11}+x^{10}+x^9+x^8+x^3+x^2+1$

Запишем вектор, чтобы посчитать.

1 1 0 1 0 0 1 0 1 0 0 1 1 1 0 0 0 0 1 1 0 1

Ошибка 1 0 0 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 0 1

Вместо 6 ошибок 3 ошибки

0 1 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0

Исходное значение синдрома

```
1 0 0 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 1 0 1 | 1 1 0 0 0 1 1 1 0 1 0 1
+ 1 1 0 0 0 1 1 1 0 1 0 1                 |-----------------------
  1 0 1 0 1 0 0 1 1 0 0 1                 | 1 1 1 0 0 1 0 0 1 1 1 1
+ 1 1 0 0 0 1 1 1 0 1 0 1
  1 1 0 1 1 1 0 1 1 0 0 1
+ 1 1 0 0 0 1 1 1 0 1 0 1
  1 0 1 1 0 1 0 1 1 0 0 0
+ 1 1 0 0 0 1 1 1 0 1 0 1
  1 1 1 0 0 1 0 1 1 0 1 1
+ 1 1 0 0 0 1 1 1 0 1 0 1
  0 1 0 0 0 0 1 0 1 1 1 0
```

Синдром: состоит из 11 разрядов: 0 1 0 0 0 0 1 0 1 1 1 0

Рассмотрим поле F_q^{r}. Тогда $n = 2^{r}-1$ Рассм. полином $(x^{n}-1)$. В данном поле этот полином раскл. на минимальные множители т.к. $g(x)$ делит $(x^{n}-1)$ без остатка, то в кач-ве $g(x)$ можно выбрать пр-ние любых минимальных множителей. При этом будет получаться порожд. полином.

Допустим, что каким-либо образом миним. множители выбраны тогда в общем случае к-ты у полинома $g(x)$ будут из поля F_q^{r}.

Если выбирать информ полиномы со к-тами из поля F_q^{r} или F_2, то при перемножении с $g(x)$ будут получ. кодовые слова, к-ты у которых в общем случае недвоичные.

Но, если выбирать $g(x)$ как миним. полином или пр-ние миним полиномов, то к-ты у $g(x)$ будут из поля F_2. Пусть все информац слова двоичные, т.е. имеют к-ты из F_2. Тогда при перемножении с $g(x)$ получаем двоичные кодовые слова и, соот-но, двоичный код

Систематический вид кода.

Пусть дана порождающая матрица G. Путем линейн преобр. её всегда можно привести к следующ. виду:

$$G = [I_k | P], \text{ где}$$

I_k - $k \times k$ единичн. матрица

P - $k \times (n-k)$

При систематич. кодировании структура кодового слова состоит из 2-х частей. Вследствии наличия единич матрицы первая часть кодового слова - это информац. блок в исходном виде, а вторая часть слова - из проверочная часть и содержит из проверочные эл-ты

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & \cdot & 0 & P_{11} & P_{12} & \dots \\ 0 & 1 & \cdot\cdot & 0 & & & \\ - & - & - & - & - & - & - \\ 0 & 0 & \cdot\cdot & 1 & P_{k1} & P_{k2} & \dots \end{array} \right)$$

$$\underbrace{\qquad\quad}_{I_k} \quad \underbrace{\qquad\quad}_{P}$$

В общем случае проверочная матрица имеет вид:

$$H = (-P^T \,;\, I_{n-k})$$

„–" – заменяется на „+" в полях Галуа по основанию 2.

~~Код циклический~~ Код, построенный по порожд. матрице G в нормальном виде, и код, построенный по матрице G в системном виде, эквивалентны.

Некоторые свойства циклических кодов.

Если задан циклич код с помощью порожд. полинома $g(x)$, длина кода равна n, тогда $k = n - \deg g(x)$

deg – степень полинома

Поэтому весь поток информации разбивается на блоки по k символов

Если код двоичный, то порожд. полином $g(x)$ имеет минимальную степень и является единственным.

Коды максимальной длины, равные длине мультипликативной группы поля назыв. кодами примитивной длины.

Введем полином $h(x) = \frac{x^n - 1}{g(x)}$ – это проверочный полином. Код, соотв. полиному $h(x)$ называется дополнительным.

По известному порожд. полиному можно построить порожд. матрицу кода. Пусть $g(x)$ имеет

к-ты g_0, g_1 и т.д. Очевидно, что максим. отлич. от нуля к-т g_{n-k}. Саму в недвоичн. коде ст- старается сделать единичным.

Набор к-тов $g(x)$, (начиная от 0-го до n), образует вектор в векторном пр-ве, где определен код. Рассм. полиномы вида $g(x), xg(x), x^2g(x), \dots, x^{k-1}g(x)$. (Набор к-тов формирует векторы, полученные циклич. вращением из предыдущ. Они линейно независимы, и могут служить базисом векторного подпр-ва, которое является кодом)

Тогда построим порожд. матрицу в виде:

$$G = \begin{pmatrix} g(x) \\ x\,g(x) \\ x^2 g(x) \\ \vdots \\ x^{k-1} g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k-1} & g_{n-k} & 0 & \dots & 0 \\ \dots & & & & & & & & \\ 0 & 0 & \dots & & & & \dots & g_{n-k-1} & g_{n-k} \end{pmatrix}$$

Данный вариант представления матрицы является не единств. возможным. Если матрица в таком виде, то можно изобразить получ. кодового слова в виде следующ. схем.

Для двоичных кодов удобно старший разряд располагать слева, тогда:

$$(\text{ст} \quad \text{мл.}) \begin{pmatrix} \text{ст} & \dots & \text{мл} \\ & \ddots & \\ & & \ddots \end{pmatrix} = (\text{ст} \dots \text{мл}).$$

Дуальный код.

Полином дуального кода можно построить по известному проверочному полиному $h(x)$ в виде:

$$b(x) = x^{\deg h(x)} \cdot h\left(\frac{1}{x}\right)$$

С помощью к-тов этого полинома также можно строить проверочную матрицу H.

Идемпотенты.

– полином $e(x)$, для которого справедливо:

$$e^2(x) = e(x).$$

Для каждого кода, опис. полиномом $g(x)$ можно выделить свой порожд. идемпотент $g(x)$. Обычно для двоичн. кодов кроме порожд. полиномов также расм. и др. полиномы, которые могут быть образующ для кода. При этом данный полином и (x^n+1) должны иметь в кач-ве наиб. общего кратного полином $g(x)$. Корни полинома $g(x)$ назыв нулями кода. Корни полинома $h(x)$ – нулями кода.

Для двоичных кодов $e(x)$ можно выразить в виде:

$$e(x) = \sum_{s \in S} \sum_{i \in C_{n,s}} x^i$$

$C_{n,s}$ – множество индексов циклотом класса,
S – все циклотом. классы,
s – подмножество циклотом. классов.

Если $e(x)$ – идемпотент и α – порожд. эл-т мультипл. группы поля, то $e(\alpha^j)$ при всех j равен „1" или „0".

Для любого циклического кода с порожд полиномом $g(x)$ можно однозначн. определить порожд. идемпотент $e(x)$ при этом идемпотент играет роль „1" в кольце, которое является кодом.
Т.к. $g(x)$ и $h(x)$ линейнонезависимы, то можно найти такие полиномы $a(x)$ и $b(x)$, что:

$$a(x)\, g(x) + b(x)\, h(x) = 1$$

Pассм. ур-ние, $^{n-1}$ $a(x)\, g(x) = e(x)$
Тогда любое кодовое слово может быть предст. в виде

$$C(x) = e(x)\, f(x)$$

Найдем $e(x)\, C(x) = e^2(x)\, f(x) = e(x)\, f(x) = C(x)$, т. е идемпотент играет роль "1".
С помощью идемпотентов удобно анализировать структуру конкретного кода, а также строить новые коды, образующиеся из исходных "кирпичи".

Разложение кодового кольца.

Возьмем в коде (кольце) произвольное под-кольцо (идеал), которое также будет кодом. Это подкольцо в свою очередь может быть описано своим порож. полиномом и идемпотентом.
Рассм. ∈ поле F_q произвольный эл-т и найдем для него миним. полином. Эл-т обозначим a, а полином - $m_a(X)$
Рассм. полином вида: $\frac{X^n - 1}{m_a(X)} = \hat{m}_a(X)$.
Этот полином может быть использован как порождающий полином для некоторого кода, который назов. миним. кодом, а соотв. идеал - минимальным идеалом.

Найдем все минимальные идеалы данного кода. Говорят, что данный код ~~будет разложимо~~ можно сконструир. с помощью миним. идеалов. Каждому миним. идеалу соотв. свой идемпотент. Пр-ние разных идеалов равно нулю. Единица кода разлагается в сумму идемпотентов миним. идеалов, которые образуют данный код

Наиболее распространенные конструкции.

1 Код пересечения двух кодов.

$$C = \{ c \in C_1 ; c \in C_2 \}$$

Код C образуется только теми вект., которые присутств. и в C_1 и в C_2.
Пусть g_1, g_2, e_1, e_2 - соот-но порожд. полиномы и идемпотенты кодов C_1, C_2. Тогда код C имеет:

$$g(x) = НОК\{ g_1(x) ; g_2(x) \};$$
$$e(x) = e_1(x)\, e_2(x).$$

2. Объединение кодов.

$$C = C_1 \oplus C_2 = \{ c_1 \in C_1, c_2 \in C_2, c = c_1 \oplus c_2 \}$$

Тогда:

$$g(x) = НОД\{ g_1(x), g_2(x) \}$$
$$e(x) = e_1(x) + e_2(x) + e_1(x)\, e_2(x)$$

Среди всех кодов можно выдел. коды, получающиеся преобразованием одного в другой. При этом если использ. след. ряд преобразований, то можно получить новый порожд. идемпотент и полином из старых.

Границы кодов

Допустим стоит задача построить код с парам. n, k, d. При этом необх. решить задачу оптимизации, напр, при заданном n постр. код с макс. k и d, или при задан. d и k минимизир. n.
Данные задачи не имеют строгого решения, но ориентиром для построения кодов служит понятие, называемое границей. Для построения границ использ. различные соображения, поэтому использ. различные виды границ

1) Граница Синглтона

Ранее было получено $n - k + 1 \geq d$.

2) Граница Гилберта.

Для кода $[n, k, d]_q$ справедливо следующее соотношение:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$$

$\lceil . \rceil$ - округление "вверх".

Для док-ва этого нерав-ва использ. проективную систему в пр-ве P^{k-1}.
Множество точек $\mathcal{P}$.
Введем в P^{k-1} гиперпл-ть H_0, в которой лежит макс кол-во точек из $\mathcal{P}$. Соотв-но по опр-ю проективной $[n, k, d]_q$ системы в H_0 лежит $(n-d)$ точек. Обозначим гиперплоскость H_0 как некое новое "проективное пр-во", размерности $(k-2)$ и обозначим P'. Т.о. получили новую $[n', k', d']_q$ систему, где $n' = n-d$, $k' = k-1$, d' опр-ся дополнительно.
В новой системе введем гиперпл-ть H', в которой лежит максимальное кол-во точек. Если рассм пр-во P^{k-1}, то в нем можно ввести $(q+1)$ гиперпл-ть, содержащ. H'.
Гиперпл-ть они одним пр-ем, а не системой, т.к. кол-во эл-тов в поле q, то дополнение на q дает гиперпл-ть. Такие все пр-во можно рассм как гиперпл-ть, содерж H'.
Очевидно, что гиперпл-ти при пересечении с H' содержат кол-во точек, меньшее, чем $(n-d)$, т к $(n-d)$ точек содержит "макс" гиперпл-ть H_0.
Из этого можно записать следующее нерав-во,

$$(q+1)(n-d) \geq \sum_{i=1}^{q+1} |\mathcal{P} \cap H'_i| = |\mathcal{P} \cap V| + q(n-d-d').$$

Рассм. лев-и пр части и получим:

$d' \ge \left\lceil \frac{d}{q} \right\rceil$

Производя последовательно аналогичные операции по уменьшению размерности пр-ва, в пределе приходим к системе $[n^{(k)}, 0, d^{(k)}]$

Очевидно, что $n^{(k)} = n - d - d' - \ldots \ge n - \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$.

Условие $n^{(k)} \ge 0$ приводит к исходному выражению.

3) Граница Плоткина

Для $[n,k,d]_q$ кода имеется ограничение "сверху" на минимальное кодовое расстояние d:

$$d \le \frac{n q^k (q-1)}{(q^k-1) q}$$

В основе данного неравенства лежит то, что d не может превосходить среднего расст. между словами

Определим $d_{ср} = \frac{1}{q^k(q^k-1)} \sum_{x,y \in C} d(x,y)$

$d(x,y)$ - расст. между двумя кодов. словами.

Определим $X_{a,i} = \{x \in C \mid x_i = a\}$ - кол-во слов x, у которых коорд. i равна a.

$$\sum_{a \in F_q} X_{a,i} = q^k.$$

Введем $\delta_{x_i,y_i} = \begin{cases} 1, & x_i = y_i \\ 0, & x_i \ne y_i \end{cases}$

Найдем сумму в исходном выражении:

$$\sum_{x,y \in C} d(x,y) = \sum_{i=1}^{n} \sum_{x,y \in C} (1 - \delta_{x_i,y_i}) = \sum_{i=1}^{n} \sum_{a,b \in F_q} (1 - \delta_{a,b}) X_{a,i} X_{b,i}$$

Найдем максимум этого выражения

Приведя такие выкладки, получим следующее выражение

$q^{2k} n \frac{q-1}{q}$ - доля ненулевых символов в поле

Полученный максимум подставь в исходное соотнош. для d и получим достаточ. условие

4) Граница Хемминга

Для любого $[n, k, d]_q$ кода выполняется

$$n - k \geq \log_q \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i$$

В основе лежит вычисление объема сферы Хемминга кодового слова для t ошибок.

Объем сферы $B_t = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$

Это объем сферы вокруг кодов слов, а точек пр-ва q^n. Тогда,

$B_t q^k \leq q^n$. Получен в данное нер-во получим исходное выражение.

Если выполн. нер-во в границе Хемминга, то кол-во точек во всех сферах равно кол-ву точек всего пр-ва, т.е достигается граница Хемминга, а код - совершенный

Границы совершен. кодов: код Голея, код Хемминга.

Семинар

Пример декодирования кода Голея.

Пусть дано кодовое слово в виде полинома.

$$X^4 + X^6 + X^7 + X^4 + X^3 + 1.$$

Внесем ошибку в слов с вектором:

01 0000000 1 0000001 00000000

Получилось следующее слово:

1001001 0000 1111110001101

При делении на $g(x)$ получ синдром: 10101111110