Прикладная Алгебра
Расширенный теормин

Затехано студентами 3 курса в разные годы

Исправленное и дополненное издание

7 января 2024 г.

1. Группы. Подгруппы и факторгруппы. Теорема Лагранжа.

Группа - тройка $\langle G, \circ, e\rangle$, где G - непустое множество, $e \in G$ - нейтральный элемент, а $\circ : G \times G \to G$ - бинарная операция, определенная на этом множестве, для которой выполняются аксиомы группы:

0. $x \circ y \in G,\ \forall x, y \in G$ - замкнутость.
1. $(x \circ y) \circ z = x \circ (y \circ z),\ \forall x, y, z \in G$ - ассоциативность.
2. $\exists e\ :\ e \circ x = x \circ e = x,\ \forall x \in G$ - свойство нейтрального элемента (наличие единицы).
3. $\forall x\ \exists y\ :\ y \circ x = x \circ y = e$ - существование обратного элемента.

Пример: группа по сложению на целых числах.

Коммутативная (абелева) группа - группа $\langle G, \circ, e\rangle$, где для операции $\circ$ выполняется свойство коммутативности: $x \circ y = y \circ x,\ \forall x, y \in G$.

Пример: группа по сложению на целых числах.

Группа **конечна**, если $|G| = n, n \in \mathbb{N}$, иначе группа **бесконечна**. Число n называется **порядком группы**.

Пример: группа по сложению на целых числах - бесконечна, по сложению модуля n конечна с порядком n.

Порядком элемента $(\mathrm{ord}(x))$ $x \in G$ называется такое минимальное число $n \in \mathbb{N}$, что $x^n = e$. Если такого числа нет, то элемент имеет бесконечный порядок.

Подгруппой группы $\langle G, \circ, e\rangle$ называется группа $\langle H, \circ, e\rangle$, где $H \subseteq G$, обозначается $H \leq G$.

Пример: $2\mathbb{Z} < \mathbb{Z}$ подгруппа четных чисел.

Одноэлементная единичная $E = \{e\}$ и вся группа называются **тривиальными подгруппами** любой группы.

Левым и правым смежными классами называются xH и Hx группы $\langle G, \circ, e\rangle$ по подгруппе H с представителем $x \in G$: $xH = \{x \circ h \mid h \in H\}$, $Hx = \{h \circ x \mid h \in H\}$

Нормальная подгруппа - такая подгруппа H группы G, что $\forall x \in G\ :\ xH = Hx$.

Фактор группой группы G по H называется множество смежных классов группы $\langle G, \circ\rangle$ по ее *нормальной* подгруппе H, с операцией $\bullet\ :\ (aH) \bullet (bH) = (a \circ b)H$. Обозначается как G/H.

Теорема Лагранжа. Порядок подгруппы H конечной группы G делит порядок самой группы: $|G| = |H| \cdot [G : H]$, где $[G : H] \in \mathbb{N}$ - **индекс** подгруппы H по группе G.
Следствие: $\mathrm{ord}(x)$ делит $|G|$

Усиление теоремы Лагранжа. Пусть m - максимальный порядок элемента в конечной *абелевой* группе G. Тогда порядок любого элемента G делит m.

Пример: $\langle\{0,1,2,3,4,5\},+_6,0\rangle$.
$\text{ord}1 = \text{ord}5 = 6,\ \ \text{ord}2 = \text{ord}4 = 3,\ \ \text{ord}3 = 2,\ \ \text{ord}0 = 1.$

Гомоморфизмом групп $\langle G,\circ,e\rangle$ и $\langle G',\cdot,e'\rangle$ называется отображение $\varphi : G \to G'$, которое сохраняет операцию, т.е. $\varphi(a\circ b) = \varphi(a)\cdot\varphi(b)$.

Изоморфизмом групп называется биективный гомоморфизм.

2. Циклические группы. Бесконечная и конечная циклические группы, количество порождающих элементов в них.

Циклической группой называется такая группа C, где каждый элемент этой группы образован некоторой целой степенью ее *образующего (порождающего)* элемента $a \in C : C = \{a^n \mid n \in \mathbb{Z}\} = \langle a\rangle$. Здесь $a^n = \underbrace{a\cdot\ldots\ldots\cdot a}_{n \text{ раз}}$, а $\cdot$ - коммутативная операция над группой.

Пример: Группа $\left\langle\frac{2\pi}{n}\right\rangle$ поворотов правильного n-угольника вокруг своего центра на указанный угол.

Циклическая группа $C = \langle a\rangle$ называется **бесконечной**, если $\text{ord}(a) = \infty$. Если же $\text{ord}(a) = n;\ n \in \mathbb{N}$, то циклическая группа называется **конечной** и $|C| = \text{ord}(a) = n$.

Любая бесконечная циклическая группа изоморфна $\mathbb{Z}$, а конечная порядка n – изоморфна $\mathbb{Z}_n$, откуда следует, что все конечные циклические группы одного порядка изоморфны друг другу.

Количество порождающих элементов в группе $\mathbb{Z}_n$ - это количество натуральных чисел, взаимно простых с n. Оно определяется функцией Эйлера $\varphi(n)$, по определению $\varphi(1) = 1$.

Т.к. любая циклическая группа порядка n изоморфна $\mathbb{Z}_n$, то она тоже имеет ровно $\varphi(n)$ порождающих элементов.

Свойства функции Эйлера (p - простое):

- $\varphi(p) = p - 1$
- $\varphi(n^k) = n^{k-1}\varphi(n) \Rightarrow \varphi(p^k) = p^{k-1}(p-1)$
- m и n - взаимно простые, $\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n)$
- $\sum\limits_{d|n}\varphi(d) = n$ ($d \mid n$ - d проходит по множителям n).

3. Кольца. Виды колец. Идеалы, главные и максимальные идеалы.

Кольцом называется абелевая группа $\langle R,+,0\rangle$, для которой определена бинарная операция умножения $\cdot$, связанная со сложением $+$ дистрибутивными законами:

- $x\cdot(y+z) = x\cdot y + x\cdot z$
- $(y+z)\cdot x = y\cdot x + z\cdot x$

Символически записывается как $\langle R, +, \cdot, 0 \rangle$.
Пример: кольцо целых чисел с обычным умножением и сложением.

Виды колец:

- Ассоциативно-коммутативное кольцо - кольцо, в котором умножение ассоциативно ($(ab)c = a(bc)$) и коммутативно ($ab = ba$). Пример: кольцо $\mathbb{Z}$; кольцо $\mathbb{Z}_n$ с $\cdot_n,\ +_n$.
- Унитальное кольцо - кольцо с нейтральным элементом (единицей) по умножению. Пример: кольцо $\mathbb{Z}_6$ вычетов.
- Тривиальное кольцо - одноэлементное множество $\{0\}$, в нем и только в нем $0 = 1$.
- Кольцо R - без делителей нуля: если из $a \cdot b = 0,\ \forall a, b \in R$ следует, что хотя бы один из сомножителей a и b равен 0. Пример: кольцо $2\mathbb{Z}$ не имеет делителей нуля, а вот кольцо квадратных матриц 2×2 имеет делители нуля:

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

- Целостное кольцо - нетривиальное унитальное ассоциативно-коммутативное кольцо без делителей нуля. Пример: кольцо $\mathbb{Z}$.

Обратимыми (не обратными!) элементами унитального коммутативного кольца называют такие элементы $a, b\ :\ a \cdot b = 1$ (не исключено $a = b$).
Пример: в кольце $\mathbb{Z}$ обратимы только порождающие элементы $+1$ и -1.

Неприводымым (неразложимым) называется такой ненулевой элемент p целостного кольца, для которого из равенства $p = a \cdot b$ следует, что либо a, либо b обратимы.
Пример: в кольце целых чисел неразложимы только простые числа и обратные к ним.

Факториальным кольцом называется такое целостное кольцо, в котором каждый ненулевой элемент либо обратим, либо однозначно представляется в виде произведения неприводимых элементов (с точностью до перестановки сомножителей и умножения на обратимые элементы).
Такое кольцо так же называют *кольцом с однозначным разложением на множители.*
Пример: кольцо $\mathbb{Z}$ факториально.

Подкольцом называется такое подмножество L кольца $\langle R, +, \cdot, 0 \rangle$, если L есть подгруппа аддитивной группы $\langle R, +, 0 \rangle$, замкнутая относительно операции умножения $\cdot$.
Пример: подкольцо четных чисел $2\mathbb{Z}$ кольца целых чисел $\mathbb{Z}$.

Собственное подкольцо - такое кольцо, которое не совпадает со всем кольцом.

Идеалом (двусторонним) называется подкольцо I коммутативного кольца $\langle R, +, \cdot, 0 \rangle$, если $\forall i \in I\ \forall r \in R\ :\ i \cdot r \in I$. Обозначается как $I \trianglelefteq R$.
Пример: все честные числа $2\mathbb{Z}$ кольца $\mathbb{Z}$.

Тривиальные идеалы - это само кольцо и его нуль 0.
Собственные идеалы - которые не совпадают со всем кольцом.

Главным и порожденным элементом $a \in R$ идеалом I, символически (a), называется такой идеал коммутативного кольца $\langle R, +, \cdot, 0, 1 \rangle$, если $I = \{a \cdot r \mid r \in R\} = (a)$.

Пример: Нулевой идеал (0); в кольце целых чисел $(n) = n\mathbb{Z}$.

Кольцами главных идеалов (КГИ) называют такие целостное кольца, в которых все идеалы главные.
Все КГИ факториальны.
Пример: кольцо $\mathbb{Z}$, все идеалы имеют вид $(n) = n\mathbb{Z}$; Кольцо $\mathbb{Z}_n$, любой идеал содержит НОД своих ненулевых элементов.

Максимальным идеалом коммутативного кольца называется всякий его идеал, который строго не содержится ни в каком другом идеале.
В нетривиальном коммутативном кольце всегда существует главный идеал.
Пример: в кольце целых чисел идеалы (2) и (3) максимальны, а (6) - нет.

4. Кольца. Классы вычетов и факторкольца. Целостные и евклидовы кольца.

Кольцом называется абелевая группа $\langle R, +, 0\rangle$, для которой определена бинарная операция умножения $\cdot$, связанная со сложением $+$ дистрибутивными законами:

- $x \cdot (y + z) = x \cdot y + x \cdot z$
- $(y + z) \cdot x = y \cdot x + z \cdot x$

Символически записывается как $\langle R, +, \cdot, 0\rangle$.

Пример: кольцо целых чисел с обычным умножением и сложением.

Идеалом называется подкольцо I коммутативного кольца $\langle R, +, \cdot, 0\rangle$, если $\forall i \in I\ \forall r \in R\ :\ i \cdot r \in I$.
Обозначается как $I \trianglelefteq R$.

Классом вычетов по модулю идеала I коммутативного кольца $\langle R, +, \cdot, 0\rangle$ с представителем r, называется множество: $r + I = \{r + i \mid r \in R,\ i \in I\} \stackrel{\text{def}}{=} \overline{r_I}$.
Классы вычетов разных представителей по модулю данного идеала либо *совпадают*, либо *не пересекаются*, а объединении дают все кольцо.

Пример: $\overline{r} = r + n\mathbb{Z} = \{r, r \pm n, r \pm 2n, \ldots\}$, где $r \in R$ - представитель из кольца R, $n \in \mathbb{N}$.

Факторкольцо - совокупность всех классов вычетов кольца R по модулю идеала I. Символически R/I.
Пример: $\mathbb{Z}/(2) = \{\overline{0}, \overline{1}\}$, здесь $\overline{0}$ - все четные числа, а $\overline{1}$ - все нечетные.

Целостное кольцо - нетривиальное унитальное ассоциативность-коммутативное кольцо без делителей нуля.
Пример: Кольцо $\mathbb{Z}$ целостно.

Евклидовым кольцом называется целостное кольцо $\langle R, +, \cdot, 0, 1\rangle$, если для каждого *ненулевого* элемента a определена *норма* $N(a) \in \mathbb{N}_0$ такая, что для любого $b \neq 0\ \exists q, r\ :\ a = q \cdot b + r$, и либо $r = 0$, либо $N(r) < N(b)$.
(Простыми словами, евклидовое кольца - такое кольцо, в котором есть деление элементов с остатком).

Пример: Кольцо целых чисел $\mathbb{Z}$, $N(a) = \text{abs}(a)$.

Иерархия колец:
ассоциативно-коммутативные → целостные → факториальные → КГИ → евклидовы → поля.

5. Поля: определение, характеристика поля, конечные и бесконечные поля. Для каких q существуют поля из q элементов? Построение расширений простых конечных полей.

Поле - целостное кольцо, в котором все ненулевые элементы обратимы.

Свойства поля:

1. ненулевые элементы поля K образуют абелеву группу K^* относительно умножения, ее называют *мультипликативной группой* данного поля.
2. факторкольцо R/I является *полем* если и только если идеал I кольца R - максимальный.
3. Любое поле имеет только два (тривиальных) идеала - $(0) = \{0\}$ и $(1) = K$.

Пример: Поле по вычету p (простое число) $\mathbb{Z}_p$.

Теорема. Мультипликативная группа K^* поля K - *циклическая*.

Примитивными элементами мультипликативной группы поля называются ее порождающие элементы. То есть, если α - примитивный элемент $\mathbb{F}_q$, то $\text{ord}(\alpha) = q - 1$ и справедливо разложение: $\mathbb{F}_q = \{0, \underbrace{\alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1} = \alpha^0 = 1}_{\mathbb{F}_q^*}\}$.

Подполем поля K называется такое поле K', которое является его подмножеством и замкнуто относительно операций поля K. Если подполе не совпадает с изначальным полем, то оно называется **собственным**.

Если у поля бесконечное количество элементов, оно называется **бесконечным полем**, иначе оно называется **конечным полем**.
Пример: Бесконечные поля и подполя - $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$; Конечные поля - $\mathbb{Z}_p$, p - простое.

Простым полем называется поле без собственного подполя.
Пример: Поле рациональных чисел $\mathbb{Q}$ – простое.

Характеристикой поля K называется порядок его аддитивной группы или наименьшее число p при котором $\underbrace{1 + \cdots + 1}_{p} = p \cdot 1 = 0$. Обозначается как $\text{char}(K) = p$.
Характеристика поля - всегда простое число, иначе если $\text{char}(K) = p = u \cdot v = (u \cdot 1) \cdot v = 0$, т.е. в поле есть делитель нуля, чего не может быть.
Если все суммы $1 + \ldots + 1$ различны, то полагают $\text{char}(K) = 0$, а не ∞.

Для каких q существуют поля из q элементов - для простых q.
Пример: $\mathbb{Z}_3$.

Простое поле Галуа - поле классов вычетов по модулю простого числа. $\mathbb{Z}/(p) \cong \mathbb{Z}_p \stackrel{\text{def}}{=} \mathbb{F}_p$, тут p - простое. Обозначается как $\mathbb{F}_p$ или $GF(p)$.

Поле K называется **расширением** поля F, если $F \subseteq K$.

Расширением простого поля называется факторкольцо $\mathbb{F}_p[x]/(a(x))$, где $\mathbb{F}_p[x]$ - кольцо всех многочленов переменной x со коэффициентами из поля $\mathbb{F}_p$, а $(a(x))$ - идеал неприводимого многочлена из кольца $\mathbb{F}_p[x]$.
Это факторкольцо по модулю идеала является *полем* относительно сложения и умножения вычетов по модулю $a(x)$. Обозначается как $\mathbb{F}_p^n$, где $n = \deg a(x)$.
Степени всех многочленов в этом поле не выше $n-1$, а их количество есть p^n.

Теорема. Любые два поля, содержащие одинаковое число элементов - изоморфны.

Для построения расширения $\mathbb{F}_p^n$ простого поля $\mathbb{F}_p$ может быть выбран любой неприводимый многочлен n-той степени из $\mathbb{F}_p[x]$.

6. Нахождение всех корней неприводимого многочлена в поле его расширения. Найти все корни многочлена $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$.

$K[x]$ - евклидово кольцо всех многочленов по формальной переменной x с коэффициентами из поля K.
Пример: $\mathbb{F}_2[x]$ - кольцо многочленов по x с коэффициентами $\{0, 1\}$

Корнем многочлена $f(x) \in K[x]$ называется такой элемент $a \in K \ : \ f(a) = 0$.
Отсюда - Найти все корни многочлена $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$.
$\mathbb{F}_2 = \{0, 1\} \Rightarrow f(0) = 1, \ f(1) = 1 \Rightarrow$ у этого многочлена в этом поле нет корней.

Неприводымым (неразложимым) многочленом над некоторым полем называется такой многочлен, который не представим в произведении двух других многочленов ненулевой степени.
Пример: многочлен из условия - $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$.

Поскольку евклидовы кольца *факториальны*, то любой многочлен разлагается в произведение неприводимых многочленов, либо сам является таковым.

- в $\mathbb{Q}$ существуют неприводимые многочлены любой степени
- в $\mathbb{R}$ линейные и квадратные с отрицательным дискриминантом
- в $\mathbb{C}$ только линейные

Теорема (о корнях неприводимого многочлена).
Пусть $\beta \in \mathbb{F}_p^n$ - корень неприводимого многочлена $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{F}_p[x]$.
Тогда $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$ - все различны и исчерпывают список *всех* n его корней и называются они *сопряженными*.
Следствие (о корнях непр. мн-чн в поле его расширения).
Если многочлен $f(x) \in \mathbb{F}_p[x]$ степени n неприводим, то $\mathbb{F}_p[x]/(f(x))$ - его поле разложения, в котором он имеет корни $x, x^p, x^{p^2}, \ldots, x^{p^{n-1}}$.

Таким образом многочлен $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ неприводимый в $\mathbb{F}_2[x]$ раскладывается в поле своего разложения $\mathbb{F}_2[x]/(f(x))$.
В этом поле $x^4 = -x - 1 = x + 1$.
А многочлен $f(x)$ имеет корни x, x^2, x^{2^2}, x^{2^3}, т.е. x, x^2, x^4, x^8.
$x = x$
$x^2 = x^2$
$x^4 = x + 1$
$x^8 = (x^4)^2 = (x + 1)^2 = x^2 + 1$

Теорема. $\forall a \in \mathbb{F}_q$ удовлетворяет равенству $x^q - x = 0$.
Следствия:

1. Каждый элемент $\mathbb{F}_p^n$ - корень $x^{p^n} - x$.
2. Каждый ненулевой элемент $\mathbb{F}_p^n$ есть корень $x^{p^n-1} - 1 = 0$. (после $\mathbb{F}_p^n$ - поле разложение бинома $x^{p^n-1} - 1$.
3. Если $n = 1$ получается док-во малой теоремы Ферма.

Теорема (о делимости биномов). В любом кольце многочленом $(x^m - 1) \mid (x^n - 1) \Leftrightarrow m \mid n$.

Теорема. Все неприводимые многочлены степени n над $\mathbb{F}_p$ делят бином $x^{p^n} - x$.

7. Минимальный многочлен элемента конечного поля и алгоритм его нахождения.

Минимальным многочленом (ММ) элемента $\beta \in \mathbb{F}_p^n$ называется нормированный многочлен (коэф. при старшей степени $\equiv 1$) $m_\beta(x) \in \mathbb{F}_p[x]$ наименьшей степени, для которого β является корнем.

В поле расширения $\mathbb{F}_p[x]/(a(x))$, где $a(x) = a_n x^n + \ldots + a_1 x + a_0$ минимальным многочленом для $\beta(x) = x$ будет $a_n^{-1} a(x)$.

Теорема (о существовании ММ). Для каждого элемента $\beta \in \mathbb{F}_p^n$ существует минимальный многочлен, и его степень не превосходит n.

Теорема (о неразложимости ММ). Минимальные многочлены неразложимы.

Теорема. Пусть $m_\beta(x)$ - минимальный многочлен для элемента β некоторого поля Галуа характеристики p, а $f(x)$ - многочлен из $\mathbb{F}_p[x]$, имеющий β своим корнем. Тогда $m_\beta(x)$ делитель $f(x)$ - $m_\beta(x) | f(x)$.
Следствие (о единственности ММ). Для каждого элемента поля существует не более одного минимального многочлена.

Примитивным многочленом называется минимальный многочлен примитивного элемента поля.

Способ нахождения минимальных многочленов. Для нахождения минимального многочлена $m_\beta(x)$ элемента $\beta \in F_p[x]/(a(x))$ вычисляем сопряженные элементы $\beta^p, \beta^{p^2}, \ldots$, пока на некотором d не окажется, что либо $\beta^{p^d} = \beta$, либо $\beta^{p^d} = x$.
Если $\beta^{p^d} = \beta$, то $m_\beta(x) = (x - \beta) \cdot (x - \beta^p) \cdot \ldots \cdot (x - \beta^{p^{d-1}})$
Если $\beta^{p^d} = x$, то $m_\beta(x)$ - это нормированный $a(x)$.

Пример: Найдем минимальные многочлены для элементов $\beta_1 = x^2 + x$ и $\beta_2 = x + 1$ поля $\mathbb{F}_2[x]/(x^4 + x + 1)$.
В этом поле $x^4 = x + 1$. Вычислим сопряженные для β_1:
$\beta_1^2 = (x^2 + x)^2 = x^4 + x^2 = x^2 + x + 1$,
$\beta_1^4 = (x^2 + x + 1)^2 = x^4 + x^2 + 1 = x + 1 + x^2 + 1 = x^2 + x = \beta_1$
Отсюда $m_{\beta_1}(x) = (x - \beta_1)(x - \beta_1^2) = x^2 + (\beta_1^2 + \beta_1)x + \beta_1^3$
$\beta_1^2 + \beta_1 = (x^2 + x + 1) + (x^2 + x) = 1$
$\beta_1^3 = (x^2 + x + 1) \cdot (x^2 + x) = \ldots = 1$
Таким образом $m_{\beta_1}(x) = x^2 + x + 1$
Теперь рассмотрим $\beta_2 = x + 1$. Найдем его сопряженные:
$\beta_2^2 = x^2 + 1$
$\beta_2^4 = x^4 + 1 = x + 1 + 1 = x$
Отсюда $m_{\beta_2}(x) = a(x) = x^4 + x + 1$.

8. Линейные коды: построение, свойства, порождающая и проверочная матрицы.

Введение в коды

Здесь и далее

- k - длина сообщения
- m - количество проверочных бит
- $n = k + m$ - длина кода

Потоковое кодирование - сообщение разбивается на блоки, каждый из которых кодируется в зависимости от предыдущих (далее такое кодирование не будет рассматриваться).

Блоковое кодирование - сообщение разбивается на блоки, каждый из которых независимо от других кодируется по одному и тому же правилу.

Пространство всех сообщений длины k - это множество $S = \{0, 1\}^k$. k называют **рангом** кода.

Для обеспечения помехозащищённости вместо сообщений передают **кодовые слова** большей длины $n = k + m, m > 0$, и поэтому такое кодирование называют **избыточным**.

Код называется **тривиальным** если $m = 0$ или $k = 0$.

Код - совокупность C всех кодовых слов. $|C| = Q = 2^k$ называется **мощностью кода**.

Кодирование - взаимно-однозначное преобразование сообщения в кодовое слово.

Кодирование при котором биты сообщения переходят в заранее фиксированные позиции кодового слова, называют **разделимым**. Тогда соответствующие k бит кодового слова называют **информационными**, а остальные m - **проверочными**.

Декодирование - восстановление сообщения по принятому, возможно искаженному кодовому слову. $R = \frac{k}{n}$ - **скорость** кода. $\frac{m}{n}$ - **избыточность кода**.

Расстояние Хэмминга - количество различных бит в двух словах одинаковой длины.

Кодовым расстоянием кода C называется минимальное хеминговое расстояние между словами этого кода. Обозначается $d(C)$ или d.

Шаром радиуса r с центром в кодовом слове называется множество всех слов, хеминговое расстояние с центром которых $\leq r$.

Сообщение - двоичный k-вектор $u = [u_0 \dots u_{k-1}] \in S = \{0,1\}^k$

Кодовое слово - двоичный n-вектор $v = [v_0 \dots v_{n-1}] \in B^n = \{0,1\}^n$

$[n,k]$-код - совокупность C всех кодовых слов.

$[n,k,d]$-код - $[n,k]$-код с кодовым расстоянием d.

Линейные коды

Линейным $[n,k]$ **кодом** называют такой блоковый (n,k)-код C, который образует линейное векторное подпространство размерности k координатного пространства W всех потенциально возможных скачанных слов. Символически $C \leq \{0,1\}^n = W$

Свойства линейного кода:

1. В двоичном случае образует абелеву группу по сложению модуля 2. Линейные двоичные коды называют *групповыми*.
2. Кодовое расстояние линейного кода - вес ненулевого слова с минимальным весом.
3. Любое кодовое слово $v \in C$ может быть представлено в виде линейной комбинации базисных вектором $v = \sum_{i=0}^{k-1} u_i g_i, \quad u_i \in \{0,1\}$. Это возможно, так как существует базис $\{g_0, g_1, \dots, g_{k-1}\}$ линейного кода C как подпространство W, где $g_i \in \{0,1\}^n$.

Систематическими кодами называются разделимые линейные коды.

Оценка Синглотна для двоичных разделимых линейных $[n,k,d]$-кодов: $d \leq n - k + 1$
Для границы Синглотна ($d = n - k + 1$) двоичных нетривиальных систематических кодов не существует.

Порождающей матрицей называется матрица $G_{k \times n}$ составленная из векторов базиса линейного кода. Она осуществляет кодирование, математически описываемое инъекцией $G : S \to \{0,1\}^n$ множества сообщений S в W: $v = uG$, где u - изначальный вектор
Пример:
$G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ - порождающая матрица, $u_1 = \begin{bmatrix} 0 & 1 \end{bmatrix}$ - сообщение,
$v_1 = u_1 G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ - кодовое слово.

Канонической формой порождающей матрицы называют форму $G = \begin{bmatrix} I_k & P_{k \times m} \end{bmatrix}$, где I_k - единичная матрица порядка k, а $P_{k \times m}$ - получившаяся матрица в ходе приведения исходной порождающей матрицы к матрице описанного вида с помощью элементарных преобразований.

Пример: матрица для кода Хэмминга строится сразу в каноническом виде.

Эквивалентными кодами называются коды, порожденные одной и той же порождающей матрицей, где по разному переставлены столбцы.

Если к порождающей матрице линейного кода добавить единичный столбец, получим **расширенный код**, в результате чего кодовые слова пополнятся битом четности, при этом код сможет обнаружить на одну ошибку больше (однако не сможет ее исправить).

Ортогональное линейное подпространство $C^\perp$ образуется всеми элементами координатного пространства W, которые ортогональны словам $[n,k]$-кода C: $C^\perp = \{w \in W \mid v \times w^T = 0\}$.
У такого кода $\dim C = k,\ \dim C^\perp = n-k = m$. При этом W не является прямой суммой C и $C^\perp$, то есть $\forall w \in W \not: w = c + c^\perp$, где $c \in C,\ c^\perp \in C^\perp$.
Элементы $C^\perp$ называют **двойственным** к C кодом.

Проверочной матрицей кода C называется матрица составленная по базису $C^\perp$. Она осуществляет сюръективное отображение $H : W \to C^\perp$.
Определена с точность до элементарного преобразования строк базисных векторов $C^\perp$.

Из выше сказанного следует следующие:
$0 \to \underbrace{\{0,1\}^k}_{S} \xrightarrow{G} \underbrace{\{0,1\}^n}_{W} \xrightarrow{H} \underbrace{\{0,1\}^{n-k}}_{C^\perp} \to 0$
При этом $\mathrm{Im}G = C = \mathrm{Ker}H$.

Вспомним: $A : X \to Y$. $\mathrm{Im}A = \{y \in Y \mid y = Ax\}$ (множество значений). $\mathrm{Ker}A = \{x \in X \mid Ax = 0\}$.

То есть $\forall u \in S\ :\ uG = v \in C \leq W,\ vH^T = Hv^T = 0 \implies GH^T = O$, где O - нулевая матрица размера $k \times m$.

$H = [P^T_{m\times k}\ I_m]$ - "Каноническая" форма *проверочной* матрицы при канонической форме порождающей матрицы $G_{k\times n} = [I_k\ P_{k\times m}]$.

Проверочная матрица переводит слова в ноль, чтобы выяснить - произошли ли ошибки в слове (0 - все хорошо, $\emptyset$ - что-то не так).

При систематическом кодировании, где сообщение попадает в последние биты кодового слова, то виды матриц следующие: $G = [P\ I],\ H = [I\ P^T]$.

Важно отметить, что линейный $[n,k]$-код может задаваться как порождающей матрицей $G_{k\times n}$, так и проверочной матрицей $H_{m\times n}$, которые определены с точностью до элементарных преобразований строк. В систематическом кодировании, когда биты фиксируются по позициям, G и H задаются однозначно.

Если в скачанном слове возникла ошибка, то есть к передаваемому слову добавился так называемый вектор ошибок e получится следующие: $w = v + e, v -$кодовое слово, $wH^T = vH^T + eH^T = 0 + eH^T \stackrel{\text{def}}{=} s$.

Синдромом слова w, принятого при передаче сообщения, закодированного линейным кодом с проверочной матрицей H и, возможно, содержащего ошибки, называют вектор $s = wH^T$.

Отметим, что даже если $s = 0$ - это не значит, что ошибок точно не произошло, возможно мы их не смогли обнаружить.

Из $eH^T = s$ следует, что e является частным решением неоднородной СЛАУ, то есть его можно найти.

Вектор ошибок восстанавливается с помощью словаря синдромов - это таблица, строки которой содержат всевозможные синдромы $s_1, \ldots, s_{2^m}$. Среди всех таких решений системы $eH^T = s$ выбирается такой, у которого наименьший вес, он называется лидером. Если таких несколько, лидером можно выбрать любой.

Дуальным (двойственным) кодом называется код, где H порождающая, а G наоборот - проверочная. Эти коды следуют из $GH^T = O = HG^T$, то есть из $[n, k]$ кода можно получить $[n, n-k]$-код.
Самодуальный код - код, у которого $H = G$.
Пример: расширенный код Хэмминга (с приписанной слева колонкой из всех единиц) самоудален.

9. Циклические коды: определение, построение, кодирование.

Циклическим кодом называется такой блоковый код, который инвариантен относительно циклических сдвигов своих кодовых слов. То есть, например, сдвиг вправо на 1 кодового слова $[0, 0, 1]$ превратит его в $[1, 0, 0]$.
Рассматривать будет непосредственно линейные циклические коды, хотя последние не обязательно являются упомянутыми.

Построение циклического кода:

1. Задаем n и выбираем любой делитель $g(x)$ степени m бинома $x^n - 1$. Многочлен $g(x)$ полностью задает циклический код, его на называют порождающим данный код или генератором этого кода. Код нетривиален при $1 < m < n$.

2. Идеал кольца $R = \mathbb{F}_2[x]/(x^n - 1)$ состоит из всех многочленов вида $f(x) \cdot g(x), \;\; 0 \le \deg f(x) < k = n - m$.

   Многочлены из этого идеала задаются *векторами своих коэффициентов, которые и будут кодовыми словами.*

Пример: Построим циклический код длины $n = 7$. Для этого выберем делитель бинома $x^7 - 1$. Разбивая $\mathbb{Z}_7$ на орбиты относительно умножения на 2 по mod 7, получим три орбиты $\{0\}, \{1, 2, 4\}, \{3, 6, 5\}$, откуда следует, что у бином $x^7 - 1$ три неприводимых неприводимых делителя - один 1ой степени, и два 3ей степени. Раскладываем его и получаем $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.
Выберем $g(x) = x^3 + x + 1$. Тогда $m = \deg g(x) = 3, \;\; k = 4$, что даст нам $[7, 4]$-код.

Кодирование циклическими кодами.
Рассматриваем циклический $[n, k]$-код C с порождающим полиномом $g(x), \;\deg g(x) = m = n - k$, делящий бином $x^n - 1$.

Несистематическое кодирование осуществляется простым умножением полинома на сообщение: $v(x) = g(x) \cdot u(x) \in C$.

Систематическое кодирование осуществляется приписыванием к сообщению в младшие разряды остатка $r(x)$ от деления $x^m u(x)$ на $g(x)$. То есть: $v(x) = x^m u(x) + r(x) = g(x)q(x)$, где $q(x)$ из $x^m u(x) = g(x)q(x) + r(x), \;\deg r(x) < m$.

Пример: Рассмотрим циклический $[7, 4]$-код и примера выше с $g(x) = x^3 + x + 1$. Попробуем закодировать $u = [0\ 0\ 1\ 1] \leftrightarrow u(x) = x^2 + x^3$.

- Несистематическое кодирование:

$$v(x) = u(x)g(x) = (x^3 + x^2)(x^3 + x + 1) = \begin{matrix} & & x^2 & & +x^4 & +x^5 & +x^6 \\ [0 & 0 & 1 & 0 & 1 & 1 & 1] \end{matrix}$$

- Систематическое кодирование:
  Находим остаток $r(x)$ от деления $x^3u(x)$ на $g(x)$: $x^3(x^3 + x^2) = (x^3 + x^2 + x)(x^3 + x + 1) + x$, здесь $r(x) = x$. Следовательно:

$$v(x) = x^3u(x) + r(x) = \begin{matrix} & x & & & & +x^5 & +x^6 \\ [0 & 1 & 0 & 0 & 0 & 1 & 1] \end{matrix}$$

Декодирование циклических кодов.
Синдромом $s(x)$ скачанного слова $w(x)$, закодированного циклическим кодом, называют остаток от деления $w(x)$ на многочлене $g(x)$, где $g(x)$ - порождает код.

Алгоритм декодирования при наличии ошибки $s(x) \neq 0$:

1. вычислить синдром $s(x)$
2. для всех 2^k возможных сообщение $u(x)$ находятся полиномы ошибок $e(x) = s(x) + g(x)u(x)$
3. из всех возможных полиномов ошибок выбирается полином $e_0(x)$ с минимальным числом одночленов. Если их несколько, то выбирается любой.
4. Восстанавливается переданное сообщение $u(x) = w(x) + e_0(x)$.

Сложность такого алгоритма декодирования экспоненциальная.

10. Действие группы на множестве. Лемма Бёрнсайда.

Пусть даны:

- группа $\langle G, \circ, e\rangle$, $|G| = n$
- множество $T, |T| = N > 0$
- $B_{ij}(T)$ - множество всех перестановок элементов T (биекций на T).
- S_T - симметрическая группа множества T: $S_T = \langle B_{ij}(T), *, 1_T\rangle$.

Два эквивалентных определения:

Определение 1. Действием α группы G на множестве T называется гомоморфизм из группы G в группу S_T.

Определение 2. $\alpha = \langle G, T, \circ, \triangleright, e, 1_T\rangle$ - двухосновная алгебра с носителями G и T, где

- $\circ : G \times G \to G$ - групповая операция
- $\triangleright : G \times T \to T$ - новая некоммутативная операция.

Аксиомы для операций:

- $e \triangleright t = t$

- $(g \circ h) \triangleright t = h \triangleright (g \triangleright t)$

Действие α группы G на множестве T называется **эффективным**, если для любых двух перестановок $g, h \in G, g \neq h$ существует элемент $t \in T$ такой, что $g(t) \neq h(t)$.
Тривиальное действие $\forall g \in G : \alpha(g) = 1_T$ неэффективно.

Отношением эквивалентности $\sim_g$ на T для перестановки g называется $t \sim_g t' \Leftrightarrow \exists k \in \mathbb{Z} : g^k(t) = t'$.

- Оно рефлексивно, симметрично и транзитивно.
- Смежные классы эквивалентности $\sim_g$ называются g-циклами. Элементы этих классов образуют циклы: $t \xrightarrow{g} t' \xrightarrow{g} \ldots \xrightarrow{g} t$.
- $v_1, v_2, \ldots, v_N$ - количества циклов длины $1, 2, \ldots, N$.
- $\langle v_1, v_2, \ldots, v_N \rangle = Type(g)$ - тип перестановки.
- $C(g)$ - число всех g-циклов.
- $C(g) = \sum\limits_{k=1}^{N} v_k(g)$ и $N = \sum\limits_{k=1}^{N} k \cdot v_k(g)$.

Пример: $T = \{1, \ldots, 10\}$ и

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 10 & 3 & 4 \end{pmatrix} = (1,9,3)(2,6)(4,8,10)(5)(7) = (2,6)(1,9,3)(4,8,10).$$

Тогда $Type(g) = \langle 2, 1, 2, 0, 0, 0, 0, 0, 0, 0 \rangle$, $C(g) = 5$, $N = 10$.

Отношением эквивалентности $\sim_G$ на T для группы G называется $t \sim_G t' \Leftrightarrow \exists g \in G : g(t) = t'$.

- Оно рефлексивно, симметрично и транзитивно.
- Классы эквивалентности $\sim_G$ называются орбитами.
- Класс эквивалентности, в которую попадает элемент t обозначается $Orb(t)$.
- Число орбит - $C(G)$

Фиксатором перестановки $g \in G$ называется множество $Fix(g) = \{t \in T : g(t) = t\} \subseteq T$.

Стабилизатором элемента $t \in T$ называется множество $Stab(t) = \{g \in G : g(t) = t\} \subseteq G$.

Лемма Бёрнсайда. Если группа G действует на множестве T, то $C(G) = \frac{1}{|G|} \sum\limits_{g \in G} |Fix(g)| = \frac{1}{|G|} \sum\limits_{t \in T} |Stab(t)|$.

11. Цикловой индекс действия группы на множестве. Вывод циклового индекса группы T правильного треугольника (S_3).

Весом $w(g)$ **перестановки** $g \in G$ называется $w(g) = x_1^{v_1} \cdot \ldots x_N^{v_N}$, где $\langle v_1, v_2, \ldots, v_N \rangle = Type(g)$.

Цикловым индексом $Z(G \underset{\alpha}{:} T, x_1, \ldots, x_N)$ действия группы G на множестве T называют средний вес подстановок в группе: $Z(G \underset{\alpha}{:} T, x_1, \ldots, x_N) = \frac{1}{|G|} \sum\limits_{g \in G} w(g) = \frac{1}{|G|} \sum\limits_{g \in G} x_1^{v_1} \cdot \ldots x_N^{v_N}$.

12. Теорема Пойа (без доказательства).

Пусть заданы множество T, группа G и действие $G \underset{\alpha}{:} T$.

1. Припишем каждому элементу из T одно из r значений (неформально: покрасим в один из r цветов). Всего, очевидно, имеется r^N раскрасок.

2. Не будем различать раскраски, если элементы t и $t' = g(t)$ раскрашены одинаково.

Тогда число неэквивалентных раскрасок равно числу классов эквивалентности и вычисляется по формуле $C(G \underset{\alpha}{:} T) = Z(G \underset{\alpha}{:} T, x_1, \ldots, x_N)\Big|_{x_1=\ldots=x_N=r}$.
Данное утверждение называется **теоремой Пойа**.

Пример. Задача о квадратах 2×2.
Сколькими способами можно раскрасить доску 2×2 в r цветов, если раскраски, переходящие друг в друга при вращении квадрата, считаются одинаковыми?

Решение:
Рассмотрим группу вращений квадрата $Z_4 = \{e, t, t^2, t^3\}$, где e - вращение квадрата на $0°$, а t - вращение на $90°$ (очевидно, что $t^4 = e$).
Рассмотрим квадрат $A = \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}$ (это не матрица, а квадрат в котором 4 ячейки под номерами 1, 2, 3 и 4!).
$eA = \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix}$, $tA = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$, $t^2A = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}$, $t^3A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$

Таким образом
$e = (1)(2)(3)(4), Type(e) = \langle 4, 0, 0, 0 \rangle, w(e) = x_1^4$
$t = (1432), Type(e) = \langle 0, 0, 0, 1 \rangle, w(e) = x_4^1$
$t^2 = (13)(24), Type(e) = \langle 0, 2, 0, 0 \rangle, w(e) = x_2^2$
$t^3 = (1234), Type(e) = \langle 0, 0, 0, 1 \rangle, w(e) = x_4^1$

Итого, цикловой индекс равен $P = \frac{1}{|G|}(x_1^4 + 2x_4^1 + x_2^2)$, подставляя $|G| = 4$ и $x_1 = x_2 = x_4 = r$, $P(r) = \frac{r^4+2r+r^2}{4}$.
Ответ: $P(r) = \frac{r^4+2r+r^2}{4}$.

13. Односторонняя функция и односторонняя функция с секретом. Электронная цифровая подпись.

Введение в криптографию

Криптография - наука о защите информации от незаконных пользователей, обеспечения целостности и реализации методов проверки подлинности.

Открытый текст - сообщение на зашифровку. Двоичное слово x длины n, то есть $x \in \{0, 1\}^n$.

Шифртекст или криптограмма - зашифрованный открытый текст.

Шифр - семейство обратимых отображений множества открытых текстов в множество шифртекстов.

Ключ или криптопеременная - параметр, обычно составной, определяющий выбор конкретного отображения из входящих в шифр, его сменная часть.

Зашифрование - процесс преобразования открытого текста в шифрованный с помощью шифра и ключа.

Расшифрование - процесс, обратный зашифрованию при известном значении ключа.

Дешифрование - процесс раскрытия криптограммы без знания секретного ключа.

Предполагается, что способ шифрования открыт.
Правило стойкости О. Керкгоффса - в секрете держится только ключ, а сам алгоритм шифрования открыт.

Шифры бывают:

- **Блочные** - сообщения разбиваются на блоки фиксированной длины и каждый шифруется независимо друг от друга.
- **Поточные** сообщение шифруется последовательно и каждый символ шифруется в зависимости от его расположение в тексте.

Асимметрическим шифрованием называется шифрование с использованием двух ключей k_e и k_d - для операций зашифрования и расшифрования соответственно. Ключ k_e называется публичным и, как правило, известен всем, а k_d называется приватным и не должен быть в открытом доступе.

Симметрическим шифрованием называется шифрование с использование единственного ключа k и понятно, что должен оставаться в секрете.

Симметрическое шифрование используют в защищенных каналах связи, асимметрическое, по причине наличия двух ключей, может использоваться и в открытых каналах. Последнее так же применяют для создания цифровой подписи или сертификата.
Как правило симметрическое шифрование быстрее асимметрического.

Полиномиальным называется алгоритм, время работы которого в зависимости от длины входного слова ограничено сверху величиной l^c для некоторой константы c не зависящей от l.

Криптостойким шифром считается такой шифр, для которого не существует метода его дешифрования, существенно более быстрого, чем полный перебор элементов пространства ключей.

Субэкспотенциальным алгоритмом называется такой алгоритм подбора ключа, что его время асимптотически меньше любой экспоненты, но больше любого полинома.

Алгоритм быстрого возведения в степень. При возведении в натуральную степень p некоторого числа используют двоичную запись *степени*: $p = p_k 2^k + p_{k-1} 2^{k-1} + \ldots + p_0 2^0,\ p_i \in \{0, 1\},\ i = \overline{0, k}$
Например для возведения в 53 степень понадобится всего 8 умножений: $a^{53} = a^{2^5} \cdot a^{2^4} \cdot a^{2^2} \cdot a^{2^0}$.

Вычисление степени по модулю в $\mathbb{F}_2$. при вычислении степени p некоторого элемента a по модулю n возводят в квадрат не само число, а его остаток от деления на n. Поэтому вычисляют вектор $[p_0 \ \dots \ p_k]$ двоичного представления p и тогда $a^p = a_0^{p_0} \cdot a_1^{p_1} \cdot \ldots \cdot a_k^{p_k} \pmod n$, где $a_0 = a,\ a_{i+1} \equiv_n a_i^2,\ i = \overline{0, k-1}$.

Малая теорема Ферма. Если целое a не делится на простое число p, то $a^{p-1} \equiv_p 1$.

Теорема Эйлера. Если $n > 1$ и $(a, n) = 1$ (a взаимно простое с n), то $a^{\varphi(n)} \equiv_n 1$.

Задача о рюкзаке. Есть рюкзак некоторого размера z, есть предметы, которые хотим в него положить. У каждого предмета есть ценность p и размере s. Необходимо загрузить рюкзак так, что стоимость предметов в нем была максимальна.

Формулировка в методичке: выбрать такие элементы из вектор-строки $a = [a_1, \dots, a_n],\ a_i \in \mathbb{Z}$ различных целых, чтобы их сумма равнялась размеру рюкзака z.

Полиномиальные алгоритмы решения задачи о рюкзаке неизвестны.

Односторонняя функция и односторонняя функция с секретом. Электронная цифровая подпись.

Односторонняя (однонаправленная) функция - такая обратимая функция $f : X \to Y$, которая обладает свойствами:

1. существует полиномиальный алгоритм вычисления значений $f(x)$,
2. Не существует полиномиального алгоритма обращения функции f (то есть способа найти f^{-1}).

До сих пор не было доказано, что такие функции существуют, и проблема их существования эквивалента проблеме $P \stackrel{?}{=} NP$

Односторонняя функция с секретом - функция $f_k(x) : X \to Y$ зависящая от параметра k, называемым *секретным ключом* или *лазейкой*; такая что:

1. вычисление значения $f_k(x)$ относительно несложно, и при этом не требуется знание параметра k,
2. вычисление значения $f_k^{-1}(y)\ \forall y \in Y$ при известном k относительно несложно,
3. нахождение $f_k^{-1}(y)$ для почти всех k и $y \in Y$ вычислительно неосуществимо без знания k.

На звание такой функции *претендует* функция $f(x) = y = x^m \mod n$ вычисления корня m-той степени по модулю n: вычисление y производится методом быстрого возведения в степень, а эффективный алгоритм обратного преобразование $f^{-1}(y)$ требует знание лазейки - примарного разложения числа n.

Криптографический протокол - набор правил, регламентирующих использование в информационных процессах криптографических преобразований и алгоритмов.

Электронная цифровая подпись (ЭЦП) - повзоляет проверить авторство документа и отсутствие в нем искажений.
Для подписания документа, его автор должен сделать следующие:

1. Вычислить значение y хэш-функции документа D.
2. Используя свой секретный ключ k к односторонней функции с секретом, автор вычисляет $x = f_k^{-1}(y)$ и посылает документ D вместе с его хэшем и вычисленным значением x.
3. Проверку авторства $f_k(x) = y$ можно провести без ключа.

14. Протокол Диффи-Хеллмана выработки общего секретного ключа по открытому каналу связи.

Протокол Диффи-Хеллмана (DH). Рассмотрим ситуацию - Алиса (A) и Боб (B) хотят обменяться секретными сообщениями по открытому каналу. Для обеспечения безопасности сообщения A и B должны выбрать общий секретный ключ.
Для этого они выбирают простое число p и некоторый элемент $\alpha \in \mathbb{F}_p$ - эти значения открыты. Затем A и B независимо выбирают $a, b \in F_p$ соответственно. Затем вычисляют α значения по mod$p$:

$$A : \mathcal{A} = \alpha^a, \quad B : \mathcal{B} = \alpha^b \tag{*}$$

После обмениваются этими значениями по открытому каналу и каждый вычисляет секретный ключ:

$$A : K = \mathcal{B}^a = \alpha^{ab} \mod p \qquad B : K = \mathcal{A}^b = \alpha^{ab} \mod p$$

Таким образом у Алисы и Боба появился общий секретный ключ, который никто кроме них не знает и который в последствии будет использоваться для симметрического шифрования.
Пассивный злоумышленник Ева (Eve, от англ. eavesdropper), перехватывающий, но не изменяющий сообщений, не может определить ключ K: его определение связано с решением одного из уравнений (*), а это вычислительно трудная задача дискретного логарифмирования.
Так же стоит отметить, что алгоритм DH не защищен от атаки man-in-the-middle: если к каналу имеет доступ *активный злоумышленник*, то ни A, ни B не могут достоверно определить, кем является их собеседник. Активный злоумышленник может вмешаться посередине открытого канала, Алисе представиться Бобом, Бобу представиться Алисой и сформировать таким образом два секретных ключа и иметь полный доступ к их переписке, соответственно делать с ней что угодно.

15. Алгоритм проверки простоты числа на основе малой теоремы Ферма.

Понятно, что самый элементарный метод проверки числа N на простоту - это поделить его на каждое число из $[2,\ \lfloor\sqrt{N}\rfloor]$. Но для больших числе это займет слишком много времени.

Малая теорема ферма. Если целое a не делится на простое число p, то $a^{p-1} \equiv_p 1$.

Тест ферма. Из интервала $[2, N-1]$ выбирается случайное число a, подчиняющееся равномерному дискретному распределению; символически $a \xleftarrow{\$} [2, N-1]$. Тогда число N *вероятно* простое, если a не делит N, то есть $a \nmid N$ и справедлива малая теорема Ферма для (a, N): $a^{N-1} \equiv_N 1$.

Число вероятно простое, так как нет полной уверенности в том, что оно простым является. Более того, существуют *числа Кармайкла*, называющиеся **псевдопростыми** - они проходят тест ферма для всех a, взаимно простых с N, однако являются составными. Благо по мере возрастания чисел Кармайкла становится меньше.

k	Число Кармайкла	Разложение
3	561	$3 \cdot 11 \cdot 17$
4	41041	$7 \cdot 11 \cdot 13 \cdot 41$
5	825265	$5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
6	321197185	$5 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 137$
7	5394826801	$7 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 67 \cdot 73$
8	232250619601	$7 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 37 \cdot 73 \cdot 163$
9	9746347772161	$7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 641$

Дополнительные вопросы (были в экзамене ранее).

16. Построение кода Хэмминга.

Плотная упаковка шаров в единичный куб. Максимальная мощность Q кода длины n, исправляющего не более $r < \lfloor n/2 \rfloor$ ошибок находится в пределах $\frac{2^n}{C_n^0+C_n^1+\ldots+C_n^{2r}} \leq Q \leq \frac{2^n}{C_n^0+C_n^1+\ldots+C_n^r}$
Граница Гильберта - нижняя граница для Q
Граница Хэмминга - верхняя граница для Q
Плотная упаковка достигается только в **совершенных** или **экстремальных кодах**.

Длина кода Хэмминга $n = 2^m - 1,\ m > 0$
Мощность $Q = \frac{2^n}{1+n}$
Код Хэмминга *линейный* и *совершенный*, исправляет одну ошибку и обнаруживает две.

Построение кода:

1. Записать единичную матрицу порядка $k = 2^m - 1 - m$.
2. Справа приписать к ней все бинарные наборы длины m где как минимум две единицы (таких будет ровно k штук).
3. Для получения кодового слова из изначальное можно:
   a) либо домножить его справа на полученную матрицу,
   b) либо приписать к матрице слева и сложить те строки, напротив которых в исходном слове стоят единицы.

Зачастую проверочную матрицу строят так, чтобы столбцы шли по возрастанию, то есть, если каждый столбец матрицы H представить как двоичное число, то матрицу упорядочивают по ним. Тогда если синдром представить как двоичное число, оно будет указывать на номер разряда, в котором произошла ошибка (разряды нумеруются с 1).

17. Определение кодов БЧХ. Пример кода длины n=15, с исправлением двух ошибок.

Коды Боуза-Чоудхри-Хоквингема (БЧХ) - циклические коды, исправляющие *не менее* заранее заданного числа ошибок.

Сопряженными элементами поля $\mathbb{F}_p^t$ называются ненулевые элементы, имеющие общий минимальный многочлен.
Циклотомический класс составлен из всех сопряженных элементов.

Циклотомические классы либо совпадают, либо не пересекаются в совокупности дают **разбиение** мультипликативной группы поля $\mathbb{F}_p^t$, или ее **разложение на классы** над $\mathbb{F}_p$.

Длина кода БЧХ определяется параметром t, $n = 2^t - 1$. Для бинома $x^n - 1$ рассматривается поле $\mathbb{F}_2^t$ его *разложения* с некоторым примитивным элементом α.
Конструктивное расстояние БЧХ кода рассчитывается по количеству исправляемых ошибок r, $\delta = 2r + 1 < n$.
Нулями кода БЧХ называются степени $\alpha, \alpha^2, \ldots, \alpha^{2r}$ примитивного элемента α поля $\mathbb{F}_2^t$.

Код БЧХ - это циклический $[n, k, d]$-код, в котором порождающий многочлен $g(x)$ является полиномом минимальной степени, имеющий корнями *все нули кода.*

Так как нули кода - корни $g(x)$, а многочлены всех кодовых слов циклического кода делятся на $g(x)$, то нули кода так же корни и многочленов кодовых слов.

Синдромами $s_1, \ldots, s_{2r}$ скачанного многочлена $w(x)$ при кодировании БЧХ-кодом с нулями $\alpha, \alpha^2, \ldots, \alpha^{2r}$ являются $s_i = w(\alpha^i),\ i = \overline{1,\ 2r}$.
Так как $w(x) = v(x) + e(x)$, где $v(x)$ - кодовое слово, $e(x)$ - вектор ошибок, то
$\forall i = \overline{1,\ 2r}\ :\ s_i = w(\alpha^i) = e(\alpha^i)$.
Очевидно, если все синдромы равны нулю, то $w(x)$ и есть кодовое слово.

Построение кода БЧХ.
Аналогично любому циклическому коду, $[n, k]$-код БЧХ задается порождающим многочленом $g(x)$, делящим бином $x^n - 1,\ k = n - \deg g(x)$.

Алгоритм построения кода БЧХ, исправляющим не менее r ошибок:

1. Выбрать параметр t таким образом, что $n = 2^t - 1 > 2r + 1 = \delta$.
2. Выбрать неприводимый многочлен $a(x)$ степени t для поля расширения $\mathbb{F}_2^t \cong \mathbb{F}_2[x]/(a(x))$.
3. Найти циклотомические классы поля $\mathbb{F}_2^t$ над $\mathbb{F}_2$. Выбрать из них те классы, в которые попадают все $2r$ нулей $\alpha, \alpha^2, \ldots, \alpha^{2r}$ кода. Пускай таких классов h.
4. Найти минимальные многочлены $g_1(x), g_2(x), \ldots, g_h(x)$ каждого выбранного класса.
5. Вычислить порождающий многочлен кода $g(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_h(x)$.

Важно отметить, что при повышении количества исправляемых ошибок при неизменной длине кода, он будет становится "хуже", например при длине кода $n = 7,\ r = 3$ получим код с 7-кратным (!) повторением.

Пример: построим код длины $n = 15$, то есть параметр $t = 4$. Рассмотрим поле $F = \mathbb{F}_2[x]/(a(x)) \cong \mathbb{F}_2^4$, где $a(x)$ некоторый неприводимый многочлен четвертой степени. Тогда мультипликативной группа $F*$ относительно своего примитивного элемента α разобьется на 5 циклотомических класса над $\mathbb{F}_2$:

$$C_0 = \{\alpha^0\},\ C_1 = \{\alpha, \alpha^2, \alpha^4, \alpha^8\},$$
$$C_2 = \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\},\ C_3 = \{\alpha^5, \alpha^{10}\},$$
$$C_4 = \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$$

В качестве неприводимого многочлена 4ой степени возьмем $a(x) = x^4 + x + 1$. Понятно, что он будет минимальным многочленом для $\alpha = x$ и всего C_1.

Допустим мы хотим исправить не менее двух ошибок, то есть $r = 2 \Rightarrow 2r = 4$, тогда нулями кода будут $\alpha, \alpha^2, \alpha^3, \alpha^4$. Как видно из построенных выше классов, нули попадают в C_1 и C_2. Найдем мм-ы для них:
1. для $g_1(x)$ вы уже нашли и он равен $a(x)$
2. а для $g_2(x)$ мм конструируется по элементам класса -
$g_2(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) = \{\dots\} = x^4 + x^3 + x^2 + x + 1.$

Отсюда порождающий многочлен кода есть
$g(x) = g_1(x) \cdot g_2(x) = x^8 + x^7 + x^6 + x^4 + 1.$

Получим, что $m = \dim g(x) = 8, \Rightarrow k = 7$. При этом $d = \delta = 5$ и мы получили БЧХ $[15, 7, 5]$-код со скоростью $7/15$.

Декодирование кодов БЧХ.
Рассматриваем $[n, k, d]$-код БЧХ, длины $n = 2^t - 1$, поле $F = \mathbb{F}_2^t = \mathbb{F}_2[x]/(a(x)), \quad \deg a(x) = t$, α - примитивный.
Пусть при передаче кодового слова произошло $\nu \le r = \lfloor (d-1)/2 \rfloor$ ошибок в позициях $j_1, \dots, j_\nu$.
Полиномом ошибок в данном случае будет $e(x) = x^{j_1} + x^{j_2} + \dots + x^{j_\nu}$.
Вычислим синдромы $s_i = w(\alpha^i) = e(\alpha^i), \ i = \overline{1,\ 2r}$ и запишем их через степени α. Предполагаем, что ошибки произошли.

$$\begin{cases} s_1 = \alpha^{j_1} + \alpha^{j_2} + \dots + \alpha^{j_\nu}, \\ s_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \dots + (\alpha^{j_\nu})^2, \\ \dots \\ s_{2r} = (\alpha^{j_1})^{2r} + (\alpha^{j_2})^{2r} + \dots + (\alpha^{j_\nu})^{2r}, \end{cases}$$

Имеем $\nu + 1$ неизвестных в данной системе - $\nu,\ j_1, \dots, j_\nu$.
Локатор ошибок, назовем так $\beta_i = \alpha^{j_i}, \ i = \overline{1, \nu}$.

$$\begin{cases} s_1 = \beta_1 + \beta_2 + \dots + \beta_\nu, \\ s_2 = (\beta_1)^2 + (\beta_2)^2 + \dots + (\beta_\nu)^2, \\ \dots \\ s_{2r} = (\beta_1)^{2r} + (\beta_2)^{2r} + \dots + (\beta_\nu)^{2r}, \end{cases}$$

Такая система задает *симметрический полином.*
Полиномом локаторов ошибок назовем $\sigma = \prod_{i=1}^{\nu} (1 + \beta_i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \dots + \sigma_\nu x^\nu$.
Формально считаем, $\sigma_0 = 1, \ \sigma_i = 0, \ i > \nu$. Понятно, что в поле $\mathbb{F}_2$ корнями такого многочлена будут $\beta^{-1} = \alpha^{-j_i}, \ i = \overline{1, \nu}$.

Теоремой Виета можем связать σ_i и β_i:

$$\begin{cases} \sigma_1 = \beta_1 + \beta_2 + \dots + \beta_\nu, \\ \sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3 + \dots + \beta_{\nu-1}\beta_\nu, \\ \dots \\ \sigma_\nu = \beta_1\beta_2 \dots \beta_\nu \end{cases}$$

Последние две системы задают величины синдромов и коэффициентов полинома локаторов ошибок как значения *симметрических полиномов*: первая - степенных сумм, вторая - элементарных. Для такого соотношения есть тождества Ньютона-Жирара, последние $2r - \nu$ из которых в нашем случае

записываются как:

$$\begin{cases} s_{\nu+1} + \sigma_1 s_\nu + \cdots + \sigma_{\nu-1} s_2 + \sigma_\nu s_1 = 0, \\ s_{\nu+2} + \sigma_1 s_{\nu+1} + \cdots + \sigma_{\nu-1} s_3 + \sigma_\nu s_2 = 0, \\ \dots \\ s_{2r} + \sigma_1 s_{2r+1} + \cdots + \sigma_{\nu-1} s_{2r-\nu+1} + \sigma_\nu s_{2r-\nu} = 0, \end{cases}$$

Эти тождества представляют собой СЛАУ относительно $\sigma_1, \dots, \sigma_\nu$, которую можно представить в виде матрицы. Стандартными методами такая система не решается, так как неизвестно значение ν.

Алгоритмы решения системы выше называются **декодерами**. Самым банальным декодером является декодер Питерсона прямого решения, который заключается в последовательном переборе всех $\nu = \overline{r, 1}$ пока матрица системы не окажется невырожденной.

Результатом работы декодера является полином локаторов ошибок $\sigma(x)$, $\nu = \deg \sigma(x)$. Но это ещё не конец, нужно отыскать все ν его корней. Для этого можно перебрать все $\alpha, \alpha^2, \dots, \alpha^n$ мультипликативной группы $\mathbb{F}^*$ и по ним найти позиции ошибок: если α^i корень, то позиция ошибки j есть $j = -i \bmod n$.

Алгоритм декодирования $[n, k, d]$-кода БЧХ.

1. Найти все синдромы $s_i = w(\alpha^i),\ i = \overline{1,\ d-1}$. Если они равны нулю, то см. последний пункт.
2. Используя декодер найти полином ошибок $\sigma(x)$, его степень - количество произошедших ошибок ν.
3. Найти все корни $\sigma(x)$, например перебором всех элементов F^*.
4. Найти позиции ошибок по степеням корней.
5. Найти полином ошибок $e(x)$ по найденным позициям и восстановить кодовое слово $v(x) = w(x) + e(x)$.
6. по $v(x)$ восстановить сообщение $u(x)$.

Более менее адекватным декодером является **декодер Сугиямы** основанный на обобщенном алгоритме Евклида.