Билет 3.1:
Циклический код как идеал

Циклический код определяется как линейное векторное подпространство $A \subset V$ — пространства всех векторов длины n над полем $GF(q)$, которое удовлетворяет циклическому сдвигу компонент своих векторов. Иными словами, если код циклический, и вектор $u = (u_0, u_1, ..., u_{n-1})$ принадлежит коду, то и вектор $u^* = (u_{n-1}, u_0, u_1, ..., u_{n-2})$ также принадлежит коду.

Идеалы кольца:

- *Определение:* Непустое подмножество κ кольца K само будет кольцом тогда и только тогда, когда:

1. κ – есть подгруппа аддитивной группы кольца, то есть когда $\forall a, b \in \kappa \to a \pm b \in \kappa$
2. $a, b \in \kappa \to a \cdot b \in \kappa$

- *Определение:* Идеалом называется такое подкольцо κ кольца K, что: $a \in \kappa, r \in K \to a \cdot r \in \kappa$

Теорема:

В кольце $\dfrac{F[x]}{x^n - 1}$ линейный код А будет циклическим тогда и только тогда, когда он идеал.

Доказательство:

Пусть код A циклический, тогда вместе с вектором $u(x)$ коду принадлежат и все сдвиги $x^i \cdot u(x), i = 1, 2, \dots, n-1$, а также все произведения $b_i \cdot x^i \cdot u(x) \in GF(q)$ и их сумма:

$$u(x) \cdot \sum_{i=0}^{n-1} b_i \cdot x^i$$

Где $u(x) \cdot \sum_{i=0}^{n-1} b_i \cdot x^i = b(x)$ – произвольный элемент кольца $\dfrac{F[x]}{x^n - 1}$. Тогда из того, что $u(x) \in A, b(x) \in \dfrac{F[x]}{x^n - 1} \Rightarrow u(x) \cdot b(x) \in A \Rightarrow A$ – идеал.

Обратно: если код A – идеал, то вместе с $u(x)$ ему принадлежит и $x \cdot u(x)$, а это и означает, что код циклический.

Билет 3.2:
Порождающий многочлен циклического кода и его свойства

Теорема:

Идеал A содержит единственный нормированный многочлен $g(x)$ минимальной степени r.

Доказательство:

Предположим противное, пусть кроме многочлена $g(x) \in A$ имеется ещё нормированный многочлен $f(x)$ той же степени. Ясно, что $g(x) \cdot f(x) \in A$, и $deg[g(x) \cdot f(x)] < r$, так как старшие коэффициенты обоих многочленов $g(x)$ и $f(x)$ одинаковы $\Longrightarrow$ противоречие.

Следствие:

Все многочлены идеала A кратны многочлену $g(x)$.

Доказательство:

Действительно, предположим противное, то есть пусть $f(x) \in A$, но $f(x) = q(x) \cdot g(x)$. Имеем последовательно: $g(x) \in A, q(x) \cdot g(x) \in A$, так как A есть идеал; $r(x) = f(x) - q(x) \cdot g(x) \in A$. Получается, что $deg[r(x)] < deg[g(x)]$, чего не может быть $\Longrightarrow r(x) = 0$

• *Определение:* Многочлен $g(x)$ называется порождающим многочленом идеала, то есть циклического кода.

Теорема:

Любой многочлен $g(x)$, порождающий идеал в кольце $\dfrac{F[x]}{x^n - 1}$, делит многочлен $x^n - 1$

Следствие:

Пусть $x^n - 1 = q(x) \cdot g(x) + r(x)$, где выполняется неравенство $deg[r(x)] < deg[(g(x)]$. Так как в кольце $\dfrac{F[x]}{x^n - 1}$ многочлен $x^n - 1$ принадлежит нулевому классу вычетов, то в нём $q(x) \cdot g(x) + r(x) = 0$, а потому $q(x) \cdot g(x) = r(x)$, и $r(x)$ принадлежит идеалу, что может быть только при $r(x) = 0$ из-за соотношения $deg[r(x)] < deg[(g(x)]$.

• *Определение:* Многочлен $h(x) = \dfrac{x^n - 1}{g(x)}$ называется проверочным многочленом идеала, то есть циклического кода.

Билет 3.3:
Порождающий многочлен с заданными свойствами

Пусть элементы

$$\alpha_1, \alpha_2, \dots, \alpha_\rho \in GF(q^m), m = 1, 2, \dots$$

корни порождающего многочлена $g(x)$ над $GF(q)$. Тогда эти же элементы являются корнями любого многочлена

$$v(x) = v_0 + v_1 \cdot x + \dots + n_{n-1} \cdot x^{n-1}$$

принадлежащего циклическому коду, порождаемому многочленом $g(x)$:

$$v(\alpha_i) = v_0 + v_1 \cdot \alpha_i + \dots + v_{n-1} \cdot \alpha_i^{n-1} = 0$$

$$((v_0, v_1, \dots, v_{n-1}), (1, \alpha_i, \dots, \alpha_i)^{n-1}) = 0$$

В билете не написано, но дополнительная информация про проверочную матрицу циклического кода.

Проверочное соотношение:

$$((v_0, v_1, \dots, v_{n-1}), (1, \alpha_i, \dots, \alpha_i)^{n-1}) = 0$$

Строки проверочной матрицы:

$$(1, \alpha_i, \dots, \alpha_i)^{n-1})$$

Проверочная матрица циклического кода:

$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_\rho & \alpha_\rho^2 & \dots & \alpha_\rho^{n-1} \end{pmatrix}$$

Билет 3.4: Важнейший класс циклических кодов (Коды БЧХ). Параметры кодов БЧХ.

- *Определение:* Кодом Боуза—Чоудхури—Хоквингема (БЧХ) над $GF(q)$ называется такой циклический код, порождающий многочлен $g(x)$ которого имеет своими корнями последовательность идущих подряд степеней некоторого произвольного элемента $\alpha \in GF(q)$:

$$\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$$

где b любое целое число и $\delta \geq 2$. Последовательность может содержать также только один элемент α^b.

Теорема про длину БЧХ кода:

Либо длина n БЧХ кода равна порядку элемента α^b, если $\delta - 2 = 0$, либо порядку элемента α в противном случае, то есть когда $\delta > 2$.

Теорема про границу БЧХ кода:

Минимальное расстояние БЧХ кода с корнями $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$ порождающего многочлена $g(x)$ равно по меньшей мере δ.

Параметры кодов БЧХ:

1. Поле элементов: $GF(q)$ – выбирается заранее
2. Поле корней $g(x)$: $GF(q^m)$ – выбирается заранее
3. Длина n: делитель $q^m - 1$ – выбирается заранее
4. Число исправляемых ошибок: t – выбирается заранее
5. Число информационный символов: $k \geq n - 2 \cdot t \cdot m \cdot (1 - \dfrac{1}{q})$
6. Лучшая оценка $k \geq n - t \cdot m$ достигается для двоичных БЧХ кодов

Билет 3.5
Декодирование БЧХ кодов (Двоичный случай, 2 ошибки)

1. Нахождение элементов поля Галуа по неприводимому многочлену.

2. Будем считать, что у нас есть вектор u (вектор u, который можно закодировать может быть длины $k = n - deg[g(x)]$), который мы закодировали путём умножения на $g(x)$. Теперь будем находить $S(\alpha_i)$ для решения данного матричного уравнения, где $S(x)$ – закодированное u, в которое внесли ошибки.

$$\begin{pmatrix} 1 & 0 & 0 \\ S_2 & S_1 & 1 \\ S_4 & S_3 & S_2 \end{pmatrix} \times \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \\ S_5 \end{pmatrix}$$

3. После нахождения $\sigma_1, \sigma_2, \sigma_3$ напишем $\sigma(z) = 1 + \sigma_1 \cdot z + \sigma_2 \cdot z^2 + \sigma_3 \cdot z^3$ и будем искать при каких α_i данное уравнение равно нулю

4. Те α_i при которых $\sigma(z) = 0$ являются обратными элементами вектора ошибок $\Longrightarrow$ надо найти обратные элементы к α_i и получим вектор ошибок.

Билет 3.6
Общий случай декодирования двоичных БЧХ-кодов (алгоритм Горенстейна-Петерсона-Цирлера)

Алгоритм:

1. Подставляя принятый вектор v корни порождающего многочлена, вычисляют элементы S_i синдрома. Если все они равны нулю, то считается, что ошибок нет и процедура окончена.
2. В противном случае из элементов синдрома составляется система уравнений и вычисляются коэффициенты $\sigma_1, \sigma_2, \ldots, \sigma_t$ многочлена локатора ошибок
3. Отыскиваются t корней многочлена локаторов ошибок последовательной подстановкой в него элементов поля $GF(q^m)$. Величины, обратные корням, есть локаторы ошибок
4. Составляется система уравнений Y_i, которая имеет единственное решение, так как е матрицы не вырождена, решением системы являются значения ошибок.
5. В соответствии с каждой нулевой парой (X_i, Y_i) из i-ого символа вектора v вычитается величина Y_i. Восстановлен передавшийся вектор u и процедура закончена.
6. Если матрица вырождена, система неразрешима, это означает, что произошло не более, чем $t-1$ ошибок. Из матрицы следует удалить последние строку и столбец, положить $\sigma_t = 0$, а из системы – последнее уравнение. Вся процедура выполняется снова после замены t на $t-1$

Теорема:

Система уравнений имеет единственное решение тогда и только тогда, когда произошло t ошибок.

Нахождение локаторов ошибок

$$\begin{pmatrix} S_t & S_{t-1} & \ldots & S_2 & S_1 \\ S_{t+1} & S_t & \ldots & S_3 & S_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{2t-1} & S_{2t-2} & \ldots & S_{t+1} & S_t \end{pmatrix} \times \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{pmatrix} = \begin{pmatrix} -S_{t+1} \\ -S_{t+2} \\ \vdots \\ -S_{-2t} \end{pmatrix}$$

Нахождение значений ошибок

1. Найти все значения σ_t, решив систему уравнений
2. Найти корни многочлена $\sigma(z) = \sigma_0 + \sigma_1 \cdot z + \cdots + \sigma_t \cdot z^t$
3. Найти локаторы $X_1, \ldots, X_t$

Вернёмся к системе уравнений на Y_i, её определитель:

$$\begin{pmatrix} X_1 & X_2 & \ldots & X_t \\ X_1^2 & X_2^2 & \ldots & X_t^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^t & X_2^t & \ldots & X_t^t \end{pmatrix} = X_1 \cdot X_2 \cdot \ldots \cdot X_t \times \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_T \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{t-1} & X_2^{t-1} & \ldots & X_t^{t-1} \end{pmatrix}$$

Справа находится определитель Вандермонда, при наличии t ошибок локаторы X_i различны, и определитель отличен от нуля, система имеет единственно решение.

Билет 3.7
Коды Рида-Соломона. Теорема о кодировании кода Рида-Соломона

• *Определение:* Кодом Рида-Соломона (РС) называется БЧХ код, если корни $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+d-2}$ его порождающего многочлена $g(x) = g_0 + g_1 \cdot x + \cdots + g_t \cdot x^r$ принадлежат тому же полю $GF(q)$, что и коэффициенты.

С другой стороны $g(x)$ – это наименьшее общее кратное минимальных функций корней. Так как $m = 1$, то минимальная функция элемента α имеет вид $m_\alpha(x) = x - \alpha$, а потому g(x) у РС-кода имеет вид:

$$g(x) = (x - \alpha^b) \cdot (x - \alpha) \cdot \ldots \cdot (x - \alpha^{b+d-2})$$

Теорема (Основное свойство РС-кода)

Код Рида-Соломона есть код МДР.

Доказательство

$$g(x) = (x - \alpha^b) \cdot (x - \alpha) \cdot \ldots \cdot (x - \alpha^{b+d-2})$$

Степень $g(x)$ равна $d - 1$, а по определению $n - k$, откуда

$$n - k = d - 1$$

• *Определение кода МДР:* Код МДР (код с максимально достижимым расстоянием) – это линейный код, для минимального расстояния которого выполняется соотношение $d = n - k + 1$, то есть код лежит на границе Синглтона.

Теорема кодирования РС-кода

Положим $a_i \in GF(q), (i = 0, 1, \ldots, k-1), \alpha \in GF(q)$, и пусть $a = (a_0, a_1, \ldots, a_{k-1})$ вектор информационных символов, а значит $a(x) = a_0 + a_1 \cdot x + \ldots + a_{k-1} \cdot x^{k-1}$ – информационный многочлен. Тогда вектором кода РС будет

$$u = (a(1), a(\alpha), \ldots, a(\alpha^{q-2}))$$

Кодировать кодом РС можно без порождающего многочлена/порождающей матрицы! Все параметры и свойства РС кода определяются полностью двумя числами: $n = q - 1$ – длиной кода и $k < n$ – числом информационных символов!

Огромное доказательство на 13-15 слайдах 9 лекции.

Билет 3.8
Алгоритм Евклида для многочленов. Расширенный алгоритм Евклида.

Алгоритм Евклида

- *Задача:* для данных многочленов $a(z), b(z)$ найти НОД$(a(z), b(z))$

Алгоритм

$a(z) = b(z) \cdot q_0(z) + r_0(z), \quad b(z) = r_0(z) \cdot q_1(z) + r_1(z)$

$r_0(z) = r_1(z) \cdot q_2(z) + r_2(z)$ $\qquad deg[b(z)] \le deg[a(z)]$

$\vdots$ $\qquad deg[r_0(z)] < deg[b(z)]$

$r_k(z) = r_{k+1}(z) \cdot q_2(z) + r_{k+2}(z)$ $\qquad deg[r_1(z)] < deg[r_0(z)]$

$\vdots$ $\qquad \vdots$

$r_{n-2}(z) = r_{n-1}(z) \cdot q_n(z)$ $\qquad deg[r_{k+2}(z)] < deg[r_{k+1}(z)]$

Откуда

$$(a(x), b(z)) = (b(z), r_0(z)) = (r_0(z), r_1(z)) = \cdots = (r_{n-1}(z), 0) = r_{n-1}(z)$$

Расширенный алгоритм Евклида

- *Задача:* для данных многочленов $a(z), b(z)$ найти такую пару многочленов $s(z), t(z)$, что

$$a(z)s(z) + b(z) \cdot t(x) = \text{НОД}(a(z), b(z))$$

Алгоритм

Запустим итерационную процедуру:

$$u_{-2}(z) = 0, u_{-1}(z) = 1$$
$$v_{-2}(z) = 1, v_{-1}(z) = 0$$

$$u_k(z) = q_k(z) \cdot u_{k-1}(z) + u_{k-2}(z)$$
$$v_k(z) = q_k(z) \cdot v_{k-1}(z) + v_{k-2}(z)$$

$$\begin{cases} v_{k-1}(z) \cdot r_k(z) + v_k(z) \cdot r_{k-1}(z) = r_{-1}(z) \\ u_{k-1}(z) \cdot r_k(z) + v_k(z) \cdot r_{k-1}(z) = r_{-2}(z) \\ v_k(z) \cdot u_{k-1}(z) - u_k(z) \cdot v_{k-1}(z) = (-1)^k \end{cases}$$

Из последней системы $\forall k \implies$:

$$r_k(z) = (-1)^k \cdot (v_k(z) \cdot r_{-2}(z) + u_k \cdot r_{-1}(z))$$

Положив $r_{-2} = a(z), \quad r_{-1}(z) = b(z)$ и $k = n - 1$ получим требуемое равенство.

Билет 3.9
Вывод ключевого уравнения для декодирования кодов Рида-Соломона

Пусть задан РС код над $GF(q)$ длины $n = q - 1$ и размерности $k < n$. Обозначения:

- $u = (u_0, u_1, ..., u_{n-1}, u_i \in GF(q)$ – кодовый вектор, переданный в канал связи
- $v = (v_0, v_1, ..., b_{n-1}), v_i \in GF(q)$ – полученный изз канала вектор, в котором могут быть ошибки
- $e = (e_0, e_1, ..., e_{n-1}), e_i \in GF(q)$ – вектор-ошибка, такой, что $v = u + e$

Синдром принятого вектора $S = (S_1, S_2, ..., S_{2\cdot t})$ имеет вид:

$$S_1 = Y_1 \cdot X_1 + Y_2 \cdot X_2 + ... + Y_t \cdot X_t$$
$$S_2 = Y_1 \cdot X_1^2 + Y_2 \cdot X_2^2 + ... + Y_t \cdot X_t^2$$
$$\vdots$$
$$S_{2\cdot t} = Y_1 \cdot X_1^{2\cdot t} + Y_2 \cdot X_2 + ... + Y_t \cdot X_t^{2\cdot t}$$

Сопоставим вектору $S = (S_1, S_2, ..., S_{2\cdot t})$ многочлен:

$$S(z) = \sum_{j=0}^{2\cdot t} S_j \cdot z^{j-1}$$

Можно показать, что:

$$S(z) = z^{2\cdot t} \cdot \sum_{i=1}^{t} Y_i \cdot X_i \cdot \frac{X_i^{2\cdot t}}{X_i \cdot z - 1} - \sum_{i=1}^{t} \frac{X_i \cdot Y_i}{X_i \cdot z - 1}$$

Полагая, что:

$$\sigma(z) = \prod_{i=1}^{t} (X_i \cdot z - 1)$$

$$\omega(z) = \sum_{i=1}^{t} Y_i \cdot X_i \cdot \prod_{l=1, l\neq i}^{t} (X_i \cdot z - 1), \quad \phi(z) = \sum_{i=1}^{t} Y_i \cdot X_i^{2\cdot t+1} \cdot \prod_{l=1, l\neq i}^{t} (X_i \cdot z - 1)$$

И получим ключевое уравнение:

$$S(z) = z^{2\cdot t} \cdot \frac{\phi(z)}{\sigma(z)} - \frac{\omega(z)}{\sigma(z)}$$

Данное уравнение можно представить в виде:

$$-\omega(z) \equiv S(z) \cdot \sigma(z) \; mod[z^{2\cdot t}]$$

В котором:

- $\omega(z)$ – многочлен значений ошибок
- $\sigma(z)$ – многочлен локаторов ошибок

Билет 3.10
Решение ключевого уравнения для декодирования кодов Рида-Соломона

Из расширенного алгоритма Евклида:

$$r_k(z) = (-1)^k \cdot (v_k(z) \cdot r_{-2}(z) + u_k \cdot r_{-1}(z))$$

или

$$r_k(z) \equiv (-1)^k \cdot u_k(z) \cdot S(z)\ mod[r_{-2}(z)]$$

Пусть $r_{-2}(z) = z^{2 \cdot t}, \quad r_{-1}(z) = S(z)$, тогда найдётся такое k, что решение сравнения

$$r_k(z) \equiv\ mod[z^{2 \cdot t}]$$

даст $\xi \cdot u_k(z) = \sigma(z), \quad (-1)^k \cdot \xi \cdot r_k(z) = \omega(z)$. k выюирается так, чтобы $r_k(z)$ был многочленом, когда впервые выполнено условие: $deg[r_k(z)] \leq t - 1$. Константа ξ выбирается так, чтобы $\sigma_0 = 1$

Теорема

При $\sigma(0) = 1$, выполнений условий $deg[\sigma(z)] \leq t$ и $deg[\omega(z)] \leq t - 1$ многочлены $\omega(z), \sigma(z)$, получаемые в качестве решения ключевого уравнения, единственны, и многочлены $\sigma(z)$ имеет минимальную степень

Дополнительная информация по нахождение значений ошибок. Формула Форни

Если

$$\sigma(z) = \prod_{i=1}^{t} (X_i \cdot z - 1) = \sum_{i=0}^{t} \sigma_i \cdot z^{i-1}$$

то

$$\sigma'(z) = \sum_{j=1}^{t} X_i \cdot \prod_{i=1, j\neq i} (X_i \cdot z - 1) = \sum_{i=1}^{t} i \cdot \sigma_i \cdot z^{i-1}$$

Подставим в

$$\omega(z) = \sum_{i=1}^{t} Y_i \cdot X_i \cdot \prod_{l=1, l\neq i}^{t} (X_i \cdot z - 1)$$

и $\sigma'(z)$ любой корень многочлена локаторов ошибок X_j^{-1}:

$$\omega(X_j^{-1}) = Y_j^{-1} \cdot \sigma'(X_j^{-1})$$

откуда

$$Y_j = \frac{\omega(X_j^{-1})}{\sigma'(X_j^{-1})}$$