Дополнительное домашнее задание
Срок сдачи: 23.12.22

1 Циклические коды

Линейный $[n, k]$-код над полем $\mathbb{F}$ называется *циклическим*, если любой сдвиг кодового слова слова также принадлежит коду, то есть

$$c = (c_0, \ldots, c_{n-1}) \in C \implies (c_{n-1}, c_0, \ldots, c_{n-1}) \in C.$$

Векторам из $\mathbb{F}^n$ будем сопоставлять многочлены из $\mathbb{F}[x]$ степени $< n$: $c_0, \ldots c_{n-1} \mapsto c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$.

1. Покажите, что циклический $[n, k]$-код C образует идеал в $F[x]/(x^n - 1)$.
2. Докажите, что код Рида-Соломона $\mathrm{RS}_{\mathbb{F}_q, \mathbb{F}_q^*}(n, d)$– циклический. Напомним, $\mathrm{RS}_{\mathbb{F}_q, \mathbb{F}_q^*}(n, d) = \{c \in \mathbb{F}_q^n \mid c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{n-k}) = 0\}$
3. Докажите, что для циклического $[n, k]$-кода C, где $k > 0$, существует единственный унитарный многочлен $g(x)$, такой что
$$c(x) \in C \iff g(x) | c(x).$$
Такой многочлен называется *порождающим*. Для него справедливо $C = \{u(x)g(x) \mid u(x) \in \mathbb{F}[x], \deg u < n - \deg g\}$.
4. Постройте порождающий многочлен для кода Рида-Соломона $\mathrm{RS}_{\mathbb{F}_q, \mathbb{F}_q^*}(n, d)$.
5. Многочлен $h(x) = \frac{x^n - 1}{g(x)}$ называется *проверочным*. Докажите, что $h(x) \in \mathbb{F}[x]/(x^n - 1)$, т.е. $g(x) | x^n - 1$.
6. Докажите обратное: если $g(x) | x^n - 1$, то множество $C = \{u(x)g(x) \mid u(x) \in \mathbb{F}[x], \deg u < n - \deg g\}$ является циклическим кодом.
7. Из многочленов g, h можно построить порождающую и проверочную матрицы:
$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & g_{n-k-1} & g_{n-k} \end{pmatrix} \qquad H = \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & 0 & 0 \\ 0 & h_k & h_{k-1} & \ldots & h_0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & h_1 & h_0 \end{pmatrix}.$$
Для циклического кода длины 7 над $\mathbb{F}_2$ с порождающим многочленом $g(x) = x^3 + x + 1$, постройте $h(x), G, H$. Каково минимальное расстояние этого кода?