

ДОМАШНЕЕ ЗАДАНИЕ № 3
Опубликовано 12.11.19, Срок сдачи: 26.11.19 (23:59)

1 Циклические коды

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

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

Векторам из \mathbb{F}^n будем сопоставлять многочлены из $\mathbb{F}[x]$ степени $< n$: $c_0, \dots, c_{n-1} \mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1}$.

- Покажите, что циклический $[n, k]$ -код C образует идеал в $\mathbb{F}[x]/(x^n - 1)$.
- Докажите, что код Рида-Соломона $\text{RS}_{\mathbb{F}_q, \mathbb{F}_q^*}(n, d)$ – циклический. Напомним, $\text{RS}_{\mathbb{F}_q, \mathbb{F}_q^*}(n, d) = \{c \in \mathbb{F}_q^n \mid c(\alpha) = c(\alpha^2) = \dots = c(\alpha^{n-k}) = 0\}$
- 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 $C = \{u(x)g(x) \mid u(x) \in \mathbb{F}[x], \deg u < n - \deg g\}$.

- Постройте порождающий многочлен для кода Рида-Соломона $\text{RS}_{\mathbb{F}_q, \mathbb{F}_q^*}(n, d)$.
- Многочлен $h(x) = \frac{x^n - 1}{g(x)}$ называется *проверочным*. Докажите, что $h(x) \in \mathbb{F}[x]/(x^n - 1)$, т.е. $g(x)|x^n - 1$.
- 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.
- Из многочленов g, h можно построить порождающую и проверочную матрицы:

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & g_{n-k-1} & g_{n-k} \end{pmatrix} \quad H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_1 & h_0 \end{pmatrix}.$$

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?