Избранные главы дискретной математики. Весна 2025г

Задачи со 2 занятия.

Решения этих задач предполагается обсудить на следующем занятии.

(1) (Аналог задачи 1 из прошлого здания.) Докажите, что в конечномерной алгебре над некоторым полем любой ненулевой элемент является либо обратимым, либо делителем нуля.

(2) На занятии была описана принципиальная схема работы устройства, называемого сдвиговым регистром с обратными связями (краткое описание см. на следующем листе), которое генерирует периодическую последовательность элементов поля вычетов по модулю p (p — простое число). Мы выяснили, что период этой последовательности определяется порядком (в группе $n \times n$-матриц) матрицы

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & a_0 \\ 1 & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & \cdots & 0 & 0 & a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}, \qquad a_0 \neq 0,$$

но для начала в качестве домашнего задания было предложено найти

а) ее характеристический многочлен $\chi_A(t) = \det(tE - A)$;

б) ее минимальный многочлен $\mu_A(t)$ (т.е. ненулевой многочлен наименьшей степени такой, что $\mu_A(A) = 0$).

Сдвиговый регистр с обратными связями.

Мы опишем принципиальную схему устройства, называемого *сдвиговым регистром с обратными связями*, но это, конечно, будет упрощенная абстрактная схема, свободная от всех возможных технических деталей. Итак, мы будем рассматривать конечную последовательность из n ячеек, в которых могут находиться координаты некоторого вектора из $\mathbb{K}^n$ (где $\mathbb{K}$ — некоторое поле), которые с каждым тактом пересчитываются по некоторым правилам, которые мы сейчас опишем. Вектор, который записан на нашем устройстве на k-ом такте, мы будем обозначать $x^{(k)} = (x_1^{(k)}, \dots, x_n^{(k)})$. Для сдвигового регистра без обратных связей правило пересчета совсем простое: все координаты сдвигаются на одну ячейку вправо, n-ая коодината теряется (например, выдается в эфир), а первая ячейка заполняется нулем: $x_1^{(k+1)} := 0$, $x_i^{(k+1)} := x_{i-1}^{(k)}$, $i = 2, \dots n$. Конечно, работа такого устройства малоинтересна: после n-го такта регистр заполнится нулями и дальше уже ничего меняться не будет. Чтобы получить что-то содержательное, добавляются обратные связи: k-я обратная связь на каждом такте прибавляет к содержимому k-ой ячейки выдаваемое в эфир значение, умноженное на некоторый постоянный коэффициент, который мы обозначим $a_{k-1} \in \mathbb{K}$, т.е. теперь формулы пересчета будут такие:

$$\begin{aligned} x_1^{(k+1)} &:= a_0 x_n^{(k)} \\ x_i^{(k+1)} &:= x_{i-1}^{(k)} + a_{i-1} x_n^{(k)} \qquad i = 2, \dots n. \end{aligned} \tag{1}$$

Нас в основном будет интересовать случай, когда $\mathbb{K}$ - конечное поле, в первых реальных приложениях, конечно, было $\mathbb{K} = \mathbb{F}_2$. В этом последнем случае обратные связи устроены особенно просто, поскольку коэффициенты a_k могут принимать всего два значения, 0 или 1, и если $a_{k-1} = 0$, то обратной связи в k-ую ячейку нет вовсе, а если $a_{k-1} = 1$, то в k-ой ячейке происходит просто суммирование двух значений: пришедшего из предыдущей ячейки и выдаваемого в эфир.

В случае конечного поля, состоящего из q элементов, в регистре может быть записано всего конечное число различных наборов, а именно q^n, поэтому не позже чем через $T \le q^n$ тактов набор значений в регистре повторится, после чего все будет повторяться с тем же периодом T, поскольку состояние регистра на следующем такте зависит только от его состояния на предыдущем. Отметим, что на самом деле период не будет превышать даже $q^n - 1$, поскольку надо еще исключить нулевой вектор: из него по формулам (1) будет и дальше получаться только нулевой вектор. Поэтому если у нас получилась какая-то периодическая последовательность с периодом, большим единицы, то нулевого вектора в этой последовательности точно нет.

Для практических приложений важно ответить на следующие два вопроса:

- При любых ли $\mathbb{K}$ и n можно подобрать обратные связи (т.е. константы $a_i \in \mathbb{K}$) таким образом, чтобы получился максимально возможный период $q^n - 1$?
- Как для этого надо подбирать эти обратные связи?

Забегая вперед скажем, что ответ на первый вопрос однозначно положительный, мы его обсудим для практически важного случая полей вычетов по модулю p. Исчерпывающего же короткого ответа на второй вопрос нет, но мы сможем описать математическую теорию, которая позволяет существенно продвинуться в этом направлении.