Избранные главы дискретной математики. Весна 2025г

Задачи с 8 занятия.

Решения этих задач предполагается обсудить на следующем занятии.

(1) Мы доказали, что любая функция $f : \mathbb{K} \to \mathbb{K}$ однозначно задается многочленом степени ниже q, где $\mathbb{K}$ — конечное поле и $q = |\mathbb{K}|$. Оказывается, если в этом утверждении заменить $\mathbb{K}$ любым конечным кольцом (коммутативным, ассоциативным и с единицей), не являющемся полем, то это утверждение будет уже неверно: докажите, что для любого конечного кольца A, не являющемся полем, существует функция $f : A \to A$, которая не задается никаким многочленом из $A[t]$. [Утешительный вариант этой задачи: докажите существование такой функции для любого кольца $A = \mathbb{Z}/n$ при составном n, или приведите пример такой функции хотя бы для какого-нибудь конечного кольца A, не являющегося полем.]

(2) Каждый булев вектор $a = (a_1, \ldots, a_m) \in \{0,1\}^m$ можно рассматривать как двоичную запись натурального числа $n_a = 2^{m-1}a_1 + 2^{m-2}a_2 + \ldots + 2a_{m-1} + a_m$, $0 \leq n_a \leq 2^{m-1}$, что задает биекцию между множеством булевых векторов $\{0,1\}^m$ и отрезком натурального ряда $[0; 2^{m-1}]$. Докажите, что при этой биекции линейный порядок на отрезке $[0; 2^{m-1}]$ соответствует лексикографическому[1] линейному порядку на множестве булевых векторов.

(3) а) Пусть p — простое число, множество функций от n переменных $\mathbb{F}_p^{\mathbb{F}_p^n}$ является p^n-мерным векторным пространством над $\mathbb{F}_p$. Для целого числа m обозначим через $[m]_p \in \mathbb{F}_p$ его класс вычетов по модулю p. Докажите, что отображение $\Psi : \mathbb{F}_p^{\mathbb{F}_p^n} \to \mathbb{F}_p^{\mathbb{F}_p^n}$, сопоставляющее функции n переменных $f : \mathbb{F}_p^n \to \mathbb{F}_p$ (т.е. $f \in \mathbb{F}_p^{\mathbb{F}_p^n}$) новую функцию

$$(\Psi f)(x_1, \ldots, x_n) = \sum_{0 \leq k_i < p} f([k_1]_p, \ldots, [k_n]_p) x_1^{k_1} \ldots x_n^{k_n},$$

является обратимым линейным оператором. [При $p \neq 2$ мне больше ничего об этом операторе неизвестно (характеристический и минимальный многочлены, собственные значения...)]

б) Докажите, что при $p = 2$ оператор Ψ является инволюцией.

в) Найдите при $p = 2$ размерность ядра и образа оператора $\Psi + \mathrm{Id}$.

г) В связи с этой задачей актуальна задача 2 из задания 3. На семинаре она еще не разбиралась, так что что она повторно предлагается для решения.

(4) На занятии был описан (без доказательства) следующий алгоритм вычисления многочлена Жегалкина булевой функции от n переменных. Задаем булеву функцию вектором из $N = 2^n$ ее значений, соответствующих лексикографическому упорядочению переменных, и записываем этот вектор в первый столбец матрицы A размером $N \times N$. Последовательно вычисляем все элементы

[1] Напомним, что отношение $\prec$ лексикографического порядка на множестве $\{0,1\}^m$ определяется так: $a = (a_1, \ldots, a_m) \prec b = (b_1, \ldots, b_m)$, если либо $a = b$, либо $\exists\ k$ такое, что $1 \leqslant k \leqslant m$ и $\forall\ i < k\ a_i = b_i$, и $a_k < b_k$. Очевидно, $\prec$ является отношением линейного порядка.

матрицы A, лежащие не ниже побочной диагонали, по столбцам, начиная со второго столбца (первый уже заполнен). Элементы столбца с номером $k+1$ вычисляются по элементам k-ого столбца по формуле $a_{i,k+1} = a_{i,k} + a_{i+1,k}$. Докажите, что после заполнения всех столбцов в первой строке матрицы A оказываются коэффициенты многочлена Жегалкина, записанные в лексикографическом порядке.

(5) Заметьте, что описанный в прошлой задаче алгоритм похож на алгоритм последовательного вычисления биномиальных коэффициентов в треугольнике Паскаля. Докажите, что если $a = (a_1, \ldots, a_m)$, $b = (b_1, \ldots, b_m)$ — два булевых вектора (т.е. $a, b \in \{0,1\}^m$), то (в обозначениях задачи 2)

$$\binom{n_a}{n_b} \equiv 1 \pmod 2 \quad \Leftrightarrow \quad a_i \geq b_i \quad \forall i.$$

(6) Попробуйте придумать обобщение утверждения предыдущей задачи для $\binom{n}{k} \pmod p$ для произвольного простого числа p.