1 Весовые характеристики функции. Сбалансированная функция. Теорема о связи множества всех отображений декартовой степени конечного множества с множеством всех систем координатных функций, следствие. Система весовых характеристик системы функций. Нормальное весовое строение системы функций. Критерий сбалансированности системы функций, следствия.

Функция $f : X \to Y$ сбалансирована, если

$$|\{x \in X \mid f(x) = y\}| = |\{x \in X \mid f(x) = z\}| \ \forall y, z \in Y. \tag{1}$$

Теорема:

$$\varphi : X^n \to X^m \iff F_{m,n} = \{f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)\} \tag{2}$$

где $F_{m,n}$ - система координатных функций.

Следствие: Множество всех отображений $V_n \to V_m$ взаимно однозначно соответствует множеству всех систем из m б.ф. от n переменных.

Весовые характеристики:

$$N^{i_1,...,i_s}_{r_1,...,r_s} = |\{(x_1, ..., x_n) \in X^n \mid f_{i_1}(x_1, ..., x_n) = r_1, ..., f_{i_s}(x_1, ..., x_n) = r_s\}| \tag{3}$$

где $\{i_1, ..., i_s\} \subseteq \{1...m\}$, $(r_1, .., r_s) \in X^s$. Множество весовых характеристик функции образуют систему весовых характеристик этой функции.

Функция имеет нормальное весовое строение (н.в.с.), если ($X = E_k$ — числа от 0 до $k-1$ (типа $\mathbb{Z}_k$)):

$$N^{i_1,...,i_s}_{r_1,...,r_s} = k^{n-s} \tag{4}$$

Теорема: Отображение $F_{m,n}$ сбалансировано $\iff$ $F_{m,n}$ имеет н.в.с.

Следствие 1: Отображение, заданное системой б.ф. $F_{m,n}$, сбалансировано $\iff$ для любого непустого подмножества $\{i_1, ..., i_s\}$ мн-ва $\{1, ..., m\}$:

$$|f_{i_1}(x_1, ..., x_n) \cdot ... \cdot f_{i_s}(x_1, ..., x_n)| = 2^{n-s} \tag{5}$$

Следствие 2: Если $F_{m,n}$ сбалансировано, то все его координатные ф-ции тоже сбалансированы.

2 Алгебраически зависимая система функций. Критерий алгебраической зависимости системы функций, следствие (без доказательства). Линейные, аффинные, нелинейные функции векторных пространств, замечания. Критерий сбалансированности линейного отображения векторных пространств (без доказательства).

Система ф-ций $F_{m,n}$ является АЗ, если $\exists b \in X$ и $\exists \psi : X^m \to X$, отличная от константы, для которых

$$\psi(f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n)) \equiv b \tag{6}$$

Теорема: Отображение φ, определяемое системой $F_{m,n}$, сюрьективно $\iff$ $F_{m,n}$ - АНЗ
Следствие: Преобразование g множества X^n биективно $\iff$ АНЗ система его координатных ф-ций.

Пусть P - некоторое поле. Ф-ция $\varphi : P^n \to P^m$ линейная, если:

$$\forall x, y \in P^n \ \forall a, b \in P : \varphi(a \cdot x + b \cdot y) = a \cdot \varphi(x) + b \cdot \varphi(y) \tag{7}$$

Ф-ция $\varphi : P^n \to P^m$ аффинная, если:

$$\varphi(x) = \psi(x) + a \tag{8}$$

где ψ - линейная функция, $a \in P^m$
Ф-ция, отличная от аффинной, назвывается нелинейной.

Утверждение: Между мн-вом линейных функций из P^n в P^m φ и мн-вом матриц $m \times n$ $_\varphi$ существует биекция. При этом коэф-ты линейного полинома i-й координатной функции соответствуют i-й строке матрицы M_φ. Верно следующее: φ сбалансирована $\iff$ $rang M_\varphi = m$.

3 Треугольное преобразование декартовой степени конечного множества. Критерий биективности треугольного преобразования, следствие. Отображение неавтономного (преобразование автономного) регистра сдвига над конечным множеством. Линейные регистры сдвига. Критерий биективности преобразования автономного регистра сдвига, следствие.

Преобразование g_n множества X^n называется треугольным, если $g_n = F_{\Delta,n} = \{f_1(x_1), f_2(x_1, x_2), ..., f_n(x_1, ..., x_n)\}$, иначе если $S(f_i) \subseteq 1, ..., i$ для $i = 1, ..., n$, где $S(f)$ — множество номеров существенных переменных функции f.
Теорема: Треугольное преобразование g_n множества X^n биективно $\iff$ функция $f_i(x_1, ..., x_i)$ биективна по последней переменной x_i, $i = 1, ..., n$.

Пусть $\tau(y_1, y_2)$ — внутренняя бинарная операция на X. Отображение ${}_f\varphi : X^{n+1} \to X^n$ называется **отображением неавтономного регистра левого сдвига над X с обратной связью** $f : X^n \to X$, если

$$ {}_f\varphi(x_1, ..., x_n, x_{n+1}) = (x_2, ..., x_n, \tau\left(f(x_1, ..., x_n), x_{n+1}\right)). \tag{9}$$

То есть, x_{n+1} нам приходит извне. Мы считаем значение функции τ от текущих элементов регистра и от новой пришедшей переменной, и ставим его на последнее (самое правое, т.к. регистр левого сдвига $\implies$ всё сдвигается влево) место.

- Число n — длина регистра.
- Отображение f — функция обратной связи.
- Переменные $x_1, ..., x_n$ — внутренние переменные.
- Переменная x_{n+1} — входная переменная.

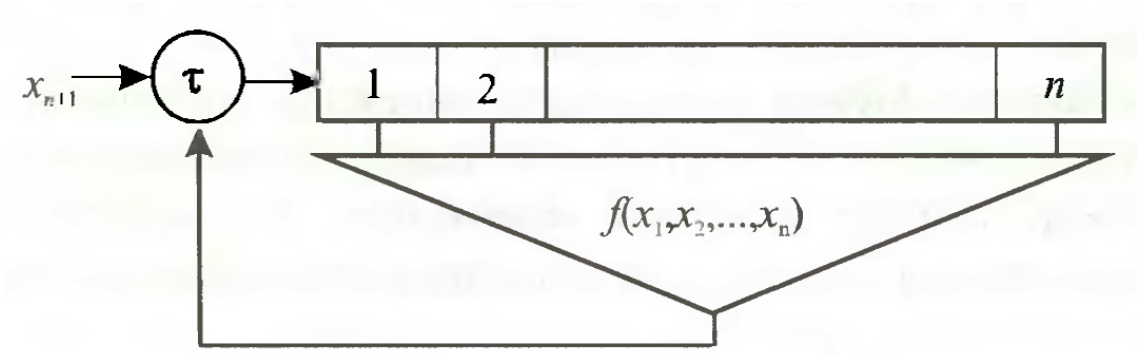

Рис. 1: Неавтономный регистр правого сдвига длины n.

Обычно X — кольцо или поле, а τ биективна по обеим переменным и реализует сложение.

Отображение регистра сдвига над кольцом X является линейным, если линейна функция обратной связи. Соответствующие регистры называются **линейными регистрами сдвига (ЛРС)** над кольцом X.

Теорема: Преобразование ${}_fg$ автономного регистра левого сдвига множества X^n биективно $\iff$ функция обратной связи $f : X^n \to X$ биективна по переменной x_1 (по выталкиваемой переменной).

Следствие: Преобразование ${}_fg$ регистра левого сдвига над $GF(2)$ с обратной связью $f : X^n \to X$ биективно $\iff$ f линейна по переменной x_1:

$$ f(x_1, ..., x_n) = x_1 \oplus \psi(x_2, ..., x_n), \tag{10}$$

где ψ — произвольная б.ф. от $n-1$ переменной.

4 Последовательность. Подпоследовательность, отрезок, мультиграмма. Функция перестановки, замены, сопряжения. Период и предпериод последовательности. Чисто периодическая последовательность. Утверждение о длинах предпериода и периода последовательности; об изменении длин периода и предпериода при замене членов последовательности.

Пусть $X_\to = \{x_1, ..., x_i, ...\}$ - бусконечная последовательность на мн-вом X порядка k.

Последовательность $\{x_{j_1}, x_{j_2}, ..., x_{j_i}, ...\}$ при $1 \le j_1 < j_2 < ... < j_i < ...$ называется подпоследовательностью пос-ти $X_\to$

Подпоследовательность $\{x_r, x_{r+1}, ..., x_{r+s-1}\}$ называется s-граммой пос-ти $X_\to$ (или $[r, r+s-1]$-отрезком $X_\to$). При $s > 1$ она называется мультиграммой.

Пос-ть $X_\to$ называется периодической, если $x_i = x_{i+\tau}$ при $i > \mu$, где $\tau \in \mathbb{N}, \mu \in \mathbb{N}_0$ (в $X_\to$ имеются совпадения на расстоянии τ, начиная с $\mu + 1$). Наименьшее такое τ называется длиной периода последовательности и обозначается через $t(X_\to)$. Длиной предпериода пос-ти ($\nu(X_\to)$) называется наименьшее $\nu \in \mathbb{N}_0$, при котором имеются совпадения на расстоянии $t(X_\to)$, начиная с номера $\nu+1$

Предпериодом называется $[1, \nu]$-отрезок, а периодом - $[\nu + i, \nu + i + t - 1]$-отрезок, $i \in \mathbb{N}$.

Чисто периодической последовательностью называется пос-ть $X_\to$, для которой $\nu(X_\to) = 0$

Утверждение:

1. Если в $X_\to$ имеются совпадения на расстоянии τ, начиная с номера $\mu + 1$, то $t \mid \tau$ и $\nu = \mu$
2. Если пос-ть $Y_\to = f^\star(X_\to) = \{f(x_i)\}$, где $X_\to = \{x_i\}$ - периодическая, а $f : X \to Y$, то Y_to - тоже периодическая, при этом: $\nu(Y_\to) \le \nu(X_\to)$ и $t(X_\to) \mid t(X_\to)$. При этом если f - биекция, то $\nu(Y_\to) = \nu(X_\to)$ и $t(X_\to) = t(X_\to)$

5 Теорема о связи длин периода и предпериода последовательностей специального вида над конечной аддитивной группой (без доказательства). Утверждение о длинах предпериода и периода сопряжения последовательностей, следствие (без доказательства). Усложненная последовательность. Верхние и нижние оценки длины периода усложненной последовательности (без доказательства).

6 Период и предпериод элемента относительно преобразования, свойства. Утверждение о связи длин периода и предпериода элемента относительно преобразования с графом преобразования, замечание (без доказательства). Период и предпериод преобразования. Утверждение о связи длин периода и предпериода преобразования с графом преобразования, замечание (без доказательства).

7 Полноцикловое преобразование. Теорема о количестве различных полноцикловых преобразований. Линейный конгруэнтный генератор (ЛКГ). ЛКГ полного периода. Критерий максимальности длины периода ЛКГ (без доказательства). Критерий полноцикловости треугольного преобразования с координатными функциями специального вида (без доказательства).

8 Принцип склеивания-расклеивания, основополагающая теорема. Линейные преобразования максимального периода. Сопровождающая матрица и характеристический многочлен линейного регистра сдвига (ЛРС). Критерий максимальности длины периода ЛРС (без доказательства). Свойства примитивных многочленов.

9 Равномерно распределенные случайные последовательности, свойства. Псевдослучайные последовательности. Рекуррентные последовательности (РП), линейные рекуррентные последовательности (ЛРП). Замечание о длине периода РП. Замечание о ĕвязи множества РП и множе-