

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, следствие.

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

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

Теорема:

$$\varphi : X^n \rightarrow X^m \iff F_{m,n} = \{f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\} \quad (2)$$

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

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

Весовые характеристики:

$$N_{r_1, \dots, r_s}^{i_1, \dots, i_s} = |\{(x_1, \dots, x_n) \in X^n \mid f_{i_1}(x_1, \dots, x_n) = r_1, \dots, f_{i_s}(x_1, \dots, x_n) = r_s\}| \quad (3)$$

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

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

$$N_{r_1, \dots, r_s}^{i_1, \dots, i_s} = k^{n-s} \quad (4)$$

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 $\{i_1, \dots, i_s\}$ мн-ва $\{1, \dots, m\}$:

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

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 $\exists \psi : X^m \rightarrow X$, отличная от константы, для которых

$$\psi(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \equiv b \quad (6)$$

Теорема: Отображение φ , определяемое системой $F_{m,n}$, сюръективно $\iff F_{m,n}$ - АНЗ

Следствие: Преобразование g множества X^n биективно \iff АНЗ система его координатных ф-ций.

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

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

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

$$\varphi(x) = \psi(x) + a \quad (8)$$

где ψ - линейная функция, $a \in P^m$

Ф-ция, отличная от аффинной, называется нелинейной.

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

3 Треугольное преобразование декартовой степени конечно-го 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 $g_n = F_{\Delta,n} = \{f_1(x_1), f_2(x_1, x_2), \dots, f_n(x_1, \dots, x_n)\}$, иначе если $S(f_i) \subseteq 1, \dots, i$ для $i = 1, \dots, n$, где $S(f)$ — множество номеров существенных переменных функции f .

Теорема: Треугольное преобразование g_n множества X^n биективно \iff функция $f_i(x_1, \dots, x_i)$ биективна по последней переменной x_i , $i = 1, \dots, n$.

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

$$f\varphi(x_1, \dots, x_n, x_{n+1}) = (x_2, \dots, x_n, \tau(f(x_1, \dots, x_n), x_{n+1})). \quad (9)$$

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 \Rightarrow всё сдвигается влево) место.

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

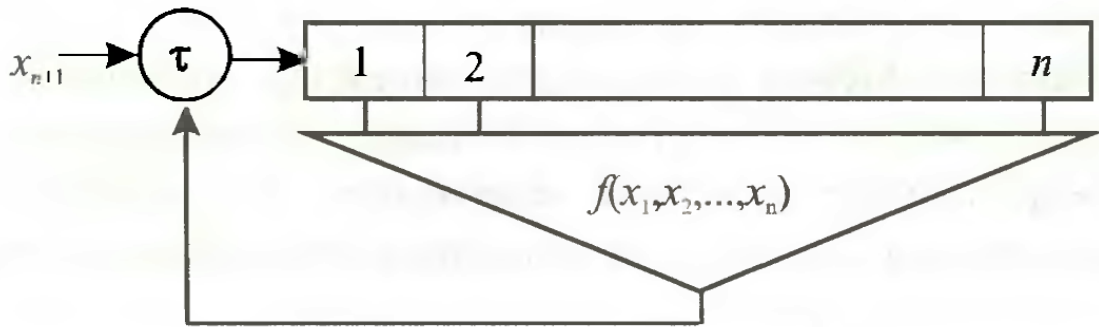


Рис. 1: Неавтономный регистр правого сдвига длины n .

Обычно X — кольцо или поле, а τ биективна по обоим 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 $f : X^n \rightarrow X$ биективна по переменной x_1 (по выталкиваемой переменной).

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

$$f(x_1, \dots, x_n) = x_1 \oplus \psi(x_2, \dots, x_n), \quad (10)$$

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.
- 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 максимальной 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 макси-