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

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

Теорема:

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

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:

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

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 $\mathbb{Z}_k$)):

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

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

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

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 $\exists \psi : X^m \to X$, 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 $\iff$ $rangM_\varphi = m$.

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.

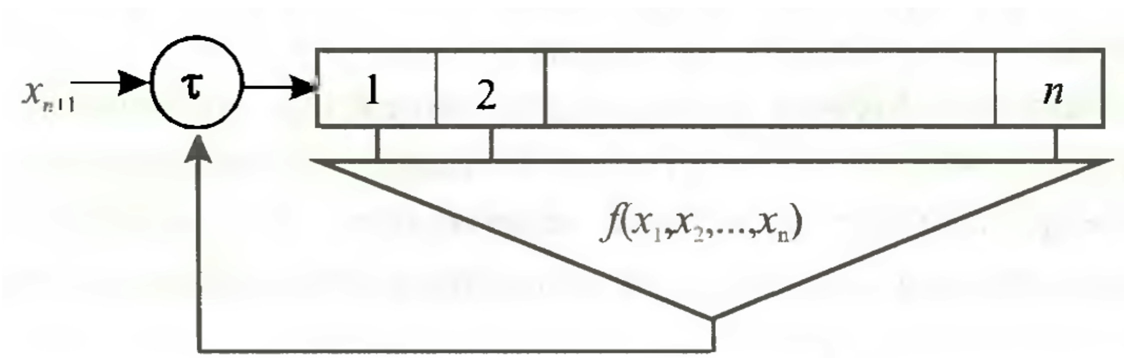

Рис. 1: Неавтономный регистр правого сдвига длины n.

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

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

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

Пос-ть $X_{\rightarrow}$ называется периодической, если $x_i = x_{i+\tau}$ при $i > \mu$, где $\tau \in \mathbb{N}, \mu \in \mathbb{N}_0$ (в $X_{\rightarrow}$ имеются совпадения на расстоянии τ, начиная с $\mu + 1$). Наименьшее такое τ называется длиной периода последовательности и обозначается через $t(X_{\rightarrow})$. Длиной предпериода пос-ти ($\nu(X_{\rightarrow})$) называется наименьшее $\nu \in \mathbb{N}_0$, при котором имеются совпадения на расстоянии $t(X_{\rightarrow})$, 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 $X_{\rightarrow}$, для которой $\nu(X_{\rightarrow}) = 0$

Утверждение:

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

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).

Теорема: Для пос-тей $X_{\rightarrow}$ и $Y_{\rightarrow}$ над конечной аддитивной группой X, где $y_i = \sum_{j=1}^{i} x_j$, выполнено:

1. Если $X_{\rightarrow}$ - периодическая с длиной предпериода $\nu > 0$ и длиной периода t, то $Y_{\rightarrow}$ - периодическая с длиной предпериода $\nu - 1$ и длиной периода t', где $t' \mid d \cdot t$, где d - порядок эл-та $y_{\nu+t} - y_{\nu}$ группы X

2. Если $X_{\to}$ - чисто периодическая с длиной периода t, то $Y_{\to}$ - чисто периодическая с длиной периода t', где $t' \mid d \cdot t$, где d - порядок эл-та y_t группы X

Утверждение:

1. $X_{\to}$ - пос-ть над $X = X_1 \times ... \times X_n$ периодическая $\iff$ $X_{\to}^{(j)}$ - периодическая $j = \overline{1, n}$. При этом верно:

$$\nu(X_{\to}) = \max\{\nu(X_{\to}^{(1)}), ..., \nu(X_{\to}^{(n)})\} \tag{11}$$

$$t(X_{\to}) = [t(X_{\to}^{(1)}), ..., t(X_{\to}^{(n)})] \tag{12}$$

2. Если пос-ть $X_{\to}^{(j)}$ отличается от $X_{\to}^{(1)}$ лишь сдвигом на $j-1$ знак, то верно:

$$\nu(X_{\to}) = \nu(X_{\to}^{(1)}) \tag{13}$$

$$t(X_{\to}) = t(X_{\to}^{(1)}) = ... = t(X_{\to}^{(n)}) \tag{14}$$

Следствие: Если $X_{\to}$ - периодическая последовательсность над $X = X_1 \times ... \times X_n$ и $t(X_{\to}) = p^m$, p - простое, $m \in \mathbb{N}$, то $t(X_{\to}^{(j)}) = p^{m_j}, j = \overline{1, n}$, где $0 \le m_j \le m$ и $\max\{m_1, ..., m_n\} = m$

Последовательсность $Y_{\to} = \{f(x_{i,1}, ..., x_{i,n})\}, i \ge 0$, полученную из пос-ти $X_{\to} = \{x_{i,1}, ..., x_{i,n}\}$ над $X = X_1 \times ... \times X_n$ с помощью ф-ции усложнения $f : X \to Y$, называются усложненной последовательностью по отношению к исходным пос-тям $X_{\to}^{(j)}, j = \overline{1, n}$.

Верхняя оценка периода $Y_{\to}$:

$$t_Y \mid [t_1, ..., t_n] \tag{15}$$

Нижние оценки:

Если $X_{1\to}$ и $X_{2\to}$ - пос-ти над аддитивной группой X с периодами t_1, t_2 соответственно, а $f(x_1, x_2) = x_1 + x_2$, то верно:

$$\frac{[t_1, t_2]}{(t_1, t_2)} \le t_Y \tag{16}$$

Если $f : X_1 \times ... \times X_n \to Y$ биективна по переменным с номерами $j_1, ..., j_b$ ($\{j_1, ..., j_b\} \subseteq \{1, ..., n\}$), то верна оценка:

$$t_Y \ge \prod_{l=1}^{b} \frac{\Theta}{\Theta_{j_l}} \tag{17}$$

где $\Theta = [t_1, ..., t_n], \Theta_j = [t_1, ..., t_{j-1}, t_{j+1}, ..., t_n], j = \overline{1, n}$

Следствие: Если f биективна по каждой переменной, а $(t_1, ..., t_n) = 1$, то длина периода $Y_{\to}$ максимальна: $t_Y = t_1 \cdot ... \cdot t_n$

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).

Пусть $g \in \Pi(X)$. $g_{\to} = \{g^i\}, i = 1, 2, ...$ - пос-ть над моноидом $\Pi(X)$, $g_{\to}(x) = \{g^i(x)\}$ - пос-ть над X.

Периодом (предпериодовм) элемента x относительно преобразования g называется период (предпериод) пос-ти $g_{\rightarrow}(x)$. Их длины обозначаются через $t_{x,g}, \nu_{x,g}$ или t_x, ν_x.

Утверждение: $\forall g \in \Pi(X), x \in X$:

$$t_{x,g} + \nu_{x,g} \leq |X| \tag{18}$$

Если x - циклическая вершина графа $\Gamma(g)$, то $\nu_{x,g} = 0, t_{x,g}$ равна длине цикла, которому принадлежит вершина x

Если x - ациклическая вершина графа $\Gamma(g)$, то $\nu_{x,g}$ равна длине подхода из x к циклу C, а $t_{x,g}$ - длина этого цикла

(Замечание ???)

Периодом (пердпериодом) преобразования g называется период (предпериод) пос-ти $g_{\rightarrow}$ (обозначение: t_g, ν_g)

Утверждение: величины t_g, ν_g - период и циклическая глубина эл-та g моноида $\Pi(X)$ $\forall g \in \Pi(X): \ t_g = [l_1, ..., l_n]$, $l_1, ..., l_n$ - длины циклов графа $\Gamma(X)$.

Если g - обратимое преобразование, то $\nu_g = 0$, иначе ν_g - наибольшая из длин подходов в графе $\Gamma(g)$

(Замечание ???)

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).

Преобразование $g \in \Pi(X)$ называется полноцикловым, если $\Gamma(g)$ представляет из себя один цикл длины n, где $n = |X|$.

Теорема: Всего различных п.ц. преобразований ровно $(n-1)!$

Преобразование $g \in \Pi(\mathbb{Z}_k)$ называется ЛКГ, если:

$$\forall x \in \mathbb{Z}_k : \ g(x) = (a \cdot x + b) \bmod k \tag{19}$$

где a, b, k - множитель, сдвиг и модуль соответственно.

Для любого k найдутся такие a, b, что ЛКГ будет преобразованием максимального периода. При этом длина периода не превышает k.

Теорема: Длина периода ЛКГ равна $k \iff$ выполнены условия:

1. $(b, k) = 1$

2. $a - 1$ делит любой простой делитель k

3. $a - 1$ делит 4, если k делит 4

В частности: $t_g = k$ при $k = 2^r \iff b$ - нечетное и $a \equiv 1 \pmod 4$

Пусть g_i - треугольная подстановка мн-ва X^i задана системой координатный ф-ций:

$$g_i = \{f_1(x_1), ..., f_i(x_1, ..., x_i)\} \tag{20}$$

Критерий: Пусть $f_i(x_1, ..., x_i) = h(x_1, ..., x_{i-1}) \oplus x_i, i = \overline{1, n}$. Треугольная подстановка g_n мн-ва X^n является полноцикловой $\iff h_1 = 1, ||h_i||$ нечетен $i = \overline{2, n}$

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 связи множества РП и множества регистров сдвига. Замечание о связи множества ЛРП и множества ЛРС.

10 ЛРП максимального периода. Характеристический многочлен ЛРП. Утверждение о количестве мультиграмм на периоде ЛРП максимального периода. Замечание о низкой стойкости ЛРП. Аннулирующий и минимальный многочлены последовательности, свойства (без доказательства). Линейная сложность последовательности. Профиль линейной сложности последовательности.

11 Утверждения о минимальном многочлене сопряжения и линейной комбинации последовательностей. Замечания о линейной сложности суммы и почленного произведения последовательностей (без доказательства). Нормальная рекуррентная последовательность. Компенсированная последовательность. Теорема о минимальном многочлене чисто периодической последовательности (без доказательства), следствие. Замечание о линейной сложности НРП (2, n) (без доказательства).

12 Поточные шифры. Синхронные поточные шифры (СПШ). Устройство СПШ. Общая и базовая схемы СПШ. Классификация СПШ по способу построения генератора