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 $\iff$ $rangM_\varphi = m$.

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.

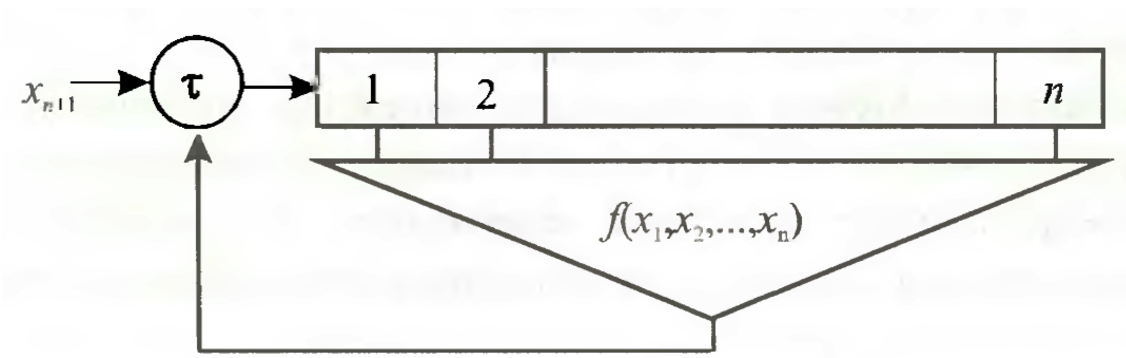

Рис. 1: Неавтономный регистр правого сдвига длины n.

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 $0 \leq m_j \leq m$ и $\max\{m_1, ..., m_n\} = m$

Последовательсность $Y_{\to} = \{f(x_{i,1}, ..., x_{i,n})\}, i \geq 0$, 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:
$$\frac{[t_1, t_2]}{(t_1, t_2)} \leq t_Y \tag{16}$$

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:
$$t_Y \geq \prod_{l=1}^{b} \frac{\Theta}{\Theta_{j_l}} \tag{17}$$
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 $g_{\to}(x)$. 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 $g_{\to}$ (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.

Теорема (принцип склеивания-расклеивания): Пусть $g,\ h$ - подстановки двоичных регистров сдвига (автономных) длины $n > 1$ и функциями обратной связи $f(x_1, ..., x_n)$ и $f(x_1, ..., x_n) \oplus x_2^{\alpha_2} \cdot ... \cdot x_n^{\alpha_n}$ соответственно, где $\alpha_2, ..., \alpha_n \in \{0, 1\}$. Тогда граф $\Gamma(g)$ отличается от графа $\Gamma(h)$ тем, что либо один цикл из $\Gamma(g)$ распадается на два цикла в $\Gamma(h)$, либо два цикла в $\Gamma(g)$ объединяются в один цикл в $\Gamma(h)$

Линейное преобразование пространства P^n, где P - поле, не может быть полноцикловым, так как нулевой элемент поля является его неподвижной точкой. Однако длина цикла в графе преобразования может составлять $k^n - 1$, где $k = |P|$. Такие преобразования называют преобразованиями максимального периода.

Рассмотрим преобразование g ЛРС (линейнго регистра сдвига) с ф-цией обратной связи $a_{n-1}x^n + ... + a_1x_2 + a_0x_1$, где $a_{n-1}, ..., a_0 \in P$. Сопровождающей матрицей данного преобразования называется матрица:

$$A_g = \begin{pmatrix} 0 & 0 & ... & 0 & a_0 \\ 1 & 0 & ... & 0 & a_1 \\ 0 & 1 & ... & 0 & a_2 \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & a_{n-1} \end{pmatrix} \tag{21}$$

Для реализации преобразования вектор $(x_1, ..., x_n)$ умножается на A_g слева. Характеристическим полиномом ЛРС называется полином:

$$F(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - ... - a_1\lambda - a_0 \tag{22}$$

A_g является корнем $F(\lambda)$. Если $F(\lambda)$ неприводим над P, то порядок матрицы совпадает с порядком полинома.

Критерий: g имеет максимальный период $\iff$ $F(\lambda)$ примитивен.

$F(\lambda)$ является неприводимым, если:

- $F(\lambda)$ неприводим над P
- $F(\lambda)$ делит полином $\lambda^{k^n-1}-1$ и не делит ни один из следующих: $\lambda^d-1, d \mid k^n-1 \wedge d \neq k^n-1$

Для полиномов над $GF(2)$ верны следующие свойства:

- Если $F(\lambda)$ степени $n>1$ неприводим над $GF(2)$, а 2^n-1 - простое число, то преобразование ЛРС мн-ва V_n имеет максимальный период
- Примитивный полином над $GF(2)$ содержит нечетное число членов
- Если $F(\lambda)$ примитивен над $GF(2)$, то примитивен над $GF(2)$ и $\lambda^n \cdot F(1/\lambda)$

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.

Случайная идеальная последовательность является реализацией последовательности независимых равномерно распределенных случайных величин. Такие последовательности называются РРСП (равномерно распределенными случайными пос-тями).

РРСП (на мн-ве X мощности k) - пос-ть $\{\zeta_1, ..., \zeta_t, ...\}$ случайных величин, принимающих значения на мн-ве X. Два требования к такой последовательности:

1. $\forall n\ \forall t_1, ..., t_n : 1 \leq t_1 < ... < t_n$ случайные величины $\zeta_{t_1}, ..., \zeta_{t_n}$ независимы в совокупности
2. $\forall t \in \mathbb{N}$ случайная величина ζ_t равномерно распределена на X

При выполнении требований справедливы свойства:

1. $\forall n\ \forall t_1, ..., t_n : 1 \leq t_1 < ... < t_n$ случайный вектор $(\zeta_{t_1}, ..., \zeta_{t_n})$ равномерно распределена на X^n
2. Воспроизводимость при прореживании: для $1 \leq t_1 < ... < t_n < ...$ соответствующая подпоследовательность $\zeta_{t_1}, ..., \zeta_{t_n}, ...$ также является РРСП
3. Воспроизводимость при суммировании: если X - аддитивная группа, а $\{\eta_t\}$ - произвольная неслучайная или произвольная случайная пос-ть над X, не зависящая от $\{\zeta_t\}$, то пос-ть $\{\zeta_t + \eta_t\}$ является РРСП.
4. $\forall t \in \mathbb{N}$ предсказание значения ζ_t по $\zeta_1, ..., \zeta_{t-1}$ невозможно, т.е. $Pr[\zeta_t = x_t \mid \zeta_1 = x_1, ..., \zeta_{t-1} = x_{t-1}] = Pr[\zeta_t = x_t] = 1/k$ для любого набора $(x_1, ..., x_t)$

Псевдослучайная последовательность (ПСП) имитирует РРСП, генерируется программным генератором (техническим устройством или программой).

Пос-ть $X_{\rightarrow}$ называется рекуррентной пос-тью (РП) порядка $n > 0$, если $\exists f : X^n \rightarrow X$

$$x_{i+n} = f(x_i, ..., x_{i+n-1}) \tag{23}$$

Равенство (23) называется законом рекурсии, f - генератором РП, а $(x_0, ..., x_{n-1})$ - начальным вектором РП. При $|X| = k$ РП порядка n обозначается как РП(k, n) Длина периода РП не превышает k^n.

Между мн-вом РП(k, n) и мн-вом регистров сдвига длины n над X существует биекция. Если генератор РП(k, n) совпадает с ф-цией обратной связи регистра сдвига, то РП(k, n) с начальным вектором $(x_0, ..., x_{n-1})$ есть первая координатная подпос-ть $X_{1\rightarrow}$ пос-ти $_fg(x_0, ..., x_{n-1})$, где $_fg$ является преобразованием X^n, реализуемое регистром

РП(k, n) над полем P называется линейной рекуррентной пос-тью (ЛРП(k, n)), если для некоторых констант $a_0, ..., a_{n-1}$ (не всех нулей) верно:

$$x_{i+n} = \sum_{j=0}^{n-1} a_j \cdot x_{i+j} \tag{24}$$

Характеристический полином ЛРП(k, n):

$$F(\lambda) = \lambda^n - a_{n-1}\lambda^{n-1} - ... - a_1\lambda - a_0 \tag{25}$$

Между мн-вом ЛРП(k, n) и мн-вом ЛРС длины n над P существует биекция. Если характеристические полиномы ЛРП(k, n) и ЛРС совпадают и равны $F(\lambda)$, то ЛРП(k, n) есть первая координатная подпос-ть пос-ти $_fg(x_0, ..., x_{n-1})$, где при $a_0 \neq 0$ $_fg$ является линейной подстановкой на P^n, реализуемая ЛРС с ф-цией обратной связи f, соответствующей характеристическому полиному $F(\lambda)$

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.

ЛРП максимального периода порождается от ненулевого начального вектора тогда и только тогда, когда ее характеристический полином примитивен

Утверждение: на периоде ЛРП длины n максимального периода над полем P порядка k всякая ненулевая s-грамма встречается k^{n-s} раз, а нулевая s-грамма встречается $k^{n-s} - 1$ раз $(1 \leq s \leq n)$

Замечание: В ЛРП(k, n) имеется простая межнаковая зависимость, позволяющая по любой n-грамме ЛРП(k, n) определить начальный вектор, решив СЛАУ.

Пусть $X_{\rightarrow}$ - пос-ть над P^m - векторны пространством над полем P. Ненулевой полином $F(\lambda)$ называется аннулирующим полиномом пос-ти $X_{\rightarrow}$, если:

$$\forall j \geq n : x_j - a_{n-1}x_{j-1} - ... - a_1 x_{j-n+1} - a_0 x_{j-n} = u \tag{26}$$

где u - нулевой элемент P^m

Минимальным полиномом $(m_{X_{\rightarrow}}(\lambda))$ называется аннулирующий полином наименьшей степени.

Свойства:

1. Если $f(\lambda) \in Ann(X_{\rightarrow})$, то $f(\lambda) \cdot g(\lambda) \in Ann(X_{\rightarrow})$ для любого ненулевого полинома $g(\lambda)$
2. Если $f_1(\lambda), ..., f_r(\lambda) \in Ann(X_{\rightarrow})$, то любая нетривиальная линейная комбинация этих полиномов над P также является аннулирующим полиномом
3. $m_{X_{\rightarrow}}(\lambda)$ определен однозначно и делит любой аннулирующий полином
4. Чисто периодическая пос-ть $X_{\rightarrow}$ с длиной периода t аннулируется полиномом $\lambda^t - 1$ и $m_{X_{\rightarrow}}(\lambda) \mid \lambda^t - 1$

Линейная сложность пос-ти $X_{\rightarrow}$:

$$\Lambda(X_{\rightarrow}) = \deg m_{X_{\rightarrow}}(\lambda) \tag{27}$$

Еще линейную сложность можно определить как порядок самой короткой ЛРП, способной породить $X_{\rightarrow}$ при некотором начальном векторе $(x_1, ..., x_{n-1})$

Профиль линейной сложности - последовательность $\{\Lambda_t\}$, где Λ_t - линейная сложность отрезка $\{x_0, ..., x_t\}$. Известно, что для случайной идеальной пос-ти: $E[\Lambda_t] \sim t/2$, $D[\Lambda_t]$ ограничена константой, убывающей с ростом порядка поля.

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 гаммы. Свойства СПШ. Атака вставкой. Необходимые условия криптографически стойкого СПШ, требования к управляющей гамме. Слабый ключ СПШ.

13 Самосинхронизирующиеся поточные шифры (ССПШ). Сходства и отличия СПШ и ССПШ. Общая схема ССПШ. Атака повторной передачи, способы защиты. Свойства ССПШ. Шифры гаммирования. Групповые шифры гаммирования, шифры модульного гаммирования. Схема алгоритма поточного шифрования A5/1.

14 Симметричные блочные шифры (СБШ). Уравнения зашифрования в режиме простой замены. Принципы построения подстановки итеративного СБШ. Раундовые ключи, раундовые функции, входное и выходное отображения, ключевое расписание. Теорема об обратимости итеративного СБШ. Замечание об «отбеливании».

15 Шифры Фейстеля, схема реализации цикловой функции. Замечание об отличии шифров Фейстеля. Замечание о биективности шифра Фейстеля. Теорема об инволютивности шифра Фейстеля, вспомогательная лемма.

16 Построение раундовой функции СБШ. Функциональ-