Лекция 11.

Периоды многочленов и ЛРП над полем. Вычисление периода неприводимого многочлена. Вычисление периода произвольного многочлена над полем по его каноническому разложению. Существование и свойства ЛРП максимального периода над конечным полем.

Напоминание: Линейные рекуррентные последовательности (ЛРП). Характеристический многочлен ЛРП.

Определение

Последовательность $u \in \mathcal{R}^\infty$ называется *линейной рекуррентной последовательностью* (или сокращённо *ЛРП*) *порядка* $m > 0$ над $\mathcal{R}$, если существуют коэффициенты $\beta_0, \ldots, \beta_{m-1} \in \mathcal{R}$ такие, что

$$u(i+m) = \beta_{m-1} u(i+m-1) + \ldots + \beta_1 u(i+1) + \beta_0 u(i) \ \forall i \in \mathbb{Z}_+. \quad (11.1)$$

Линейные рекуррентные последовательности (ЛРП). Характеристический многочлен ЛРП.

Определение

Соотношение (11.1) называют *законом рекурсии* ЛРП u, многочлен $F(x) = x^m - \beta_{m-1}x^{m-1} - \ldots - \beta_1 x - \beta_0 \in \mathcal{R}[x]$ — её *характеристическим многочленом*, а вектор $u(\overline{0, m-1}) = (u(0), \ldots, u(m-1)) \in \mathcal{R}^m$ — *начальным вектором* ЛРП u. По определению также считаем, что нулевая последовательность (0) —ЛРП порядка 0 с характеристическим многочленом $F(x) = 1$, и (0) — единственная ЛРП порядка 0.

Напоминание:Пространство последовательностей над кольцом как модуль над кольцом многочленов.

Следующая теорема показывает, что $\mathcal{R}[x]$-модуль $L_{\mathcal{R}}(F)$ является циклическим, т.е. для его задания достаточно одной последовательности.

Теорема

Пусть $F(x) = x^m - \beta_{m-1}x^{m-1} - \ldots - \beta_1 x - \beta_0 \in \mathcal{R}[x]$, $m > 0$. Через $e^F \in L_{\mathcal{R}}(F)$ обозначим ЛРП с начальным вектором $e_m = (0, \ldots, 0, 1)$. Тогда для любой последовательности $u \in L_{\mathcal{R}}(F)$ существует единственный многочлен $\Phi(x) \in \mathcal{R}[x]$ степени $\deg \Phi(x) < m$ такой, что $u = \Phi(x) \cdot e^F$, имеющий вид

$$\Phi(x) = u(0)x^{m-1} + \sum_{k=1}^{m-1}(u(k) - \beta_{m-1}u(k-1) - \ldots$$

$$\ldots - \beta_{m-k}u(0))x^{m-1-k}. \quad (11.2)$$

Напоминание: Импульсная последовательность. Генератор ЛРП.

Определение

Последовательность $e^F \in L_{\mathcal{R}}(F)$ называется *импульсной последовательностью*. Многочлен $\Phi(X)$, определённый равенством (11.2), называется *генератором ЛРП и относительно её характеристического многочлена $F(x)$.*

Напоминание: Минимальный многочлен ЛРП.

Определение

Минимальным многочленом ЛРП u называется её характеристический многочлен, имеющий наименьшую степень. Степень минимального многочлена называется ***рангом*** ЛРП u.

Из этого определения видно, что ранг u определён однозначно, поэтому корректно использовать обозначение $\mathrm{rk}\, u$. В то же время, ЛРП над кольцом может иметь несколько минимальных многочленов.

Напоминание: Минимальный многочлен ЛРП над полем и его свойства. Аннулятор ЛРП.

Определение

Аннулятором последовательности $u \in \mathcal{R}^\infty$ называется множество

$$\mathrm{ann}(u) = \{H(x) \in \mathcal{R}[x] : \; H(x) \cdot u = 0\}.$$

Заметим некоторые очевидные свойства аннулятора последовательности:

Предложение

1. $\mathrm{ann}(u)$ является идеалом кольца $\mathcal{R}[x]$;
2. $u \in \mathcal{R}^\infty$ является ЛРП над $\mathcal{R}$ тогда и только тогда, когда $\mathrm{ann}(u)$ содержит унитарный многочлен;
3. Минимальным многочленом ЛРП u является любой унитарный многочлен наименьшей степени из $\mathrm{ann}(u)$.

Напоминание: Единственность минимального многочлена ЛРП над полем.

Теорема

Любая ЛРП u над полем $\mathbb{F}$ имеет единственный минимальный многочлен $M_u(x) \in \mathbb{F}[x]$. Кроме того, он удовлетворяет равенству

$$\mathrm{ann}(u) = \mathbb{F}[x]M_u(x),$$

т.е. является образующим элементом идеала $\mathrm{ann}(u)$, и соответственно, делит все характеристические многочлены ЛРП u.

Напоминание: Нахождение минимального многочлена ЛРП.

Следствие

Для любого унитарного многочлена $F(x) \in \mathcal{R}[x]$ справедливо равенство $\mathrm{ann}(e^F) = \mathcal{R}[x]F(x)$.

Следующая теорема даёт способ нахождения минимального многочлена ЛРП над полем.

Теорема

Пусть u — ЛРП над полем $\mathbb{F}$ с характеристическим многочленом $F(x)$ и генератором $\Phi(x)$. Тогда

1. $M_u(x) = \dfrac{F(x)}{(F(x), \Phi(x))}$;
2. если $v = H(x) \cdot u$ для некоторого $H(x) \in \mathbb{F}[x]$, то $M_v(x) = \dfrac{M_u(x)}{(H(x), M_u(x))}$.

Пусть Ω — произвольное множество.

Определение

Последовательность $u \in \Omega^{\infty}$ называется *периодической*, если существуют индексы $\lambda \in \mathbb{Z}_{+}$, $t \in \mathbb{N}$ такие, что

$$u(i+t) = u(i) \ \forall i \geqslant \lambda. \tag{11.3}$$

Напоминание: Связь с ЛРП.

Пусть $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$.
Заметим очевидную связь периодических последовательностей и ЛРП над кольцом:

Предложение

Пусть $u \in \mathcal{R}^{\infty}$. Тогда
1. условие (11.3) эквивалентно условию

$$x^{\lambda}(x^{t} - 1) \cdot u = (0); \tag{11.4}$$

2. если u — периодическая, то u является ЛРП над кольцом $\mathcal{R}$.

Напоминание: Общие свойства и параметры периодических последовательностей.

Пусть $u \in \Omega^\infty$ — периодическая последовательность. Очевидно, что для неё существует не один набор параметров (λ, t), для которых выполнено равенство (11.3). Для того, чтобы описать все такие параметры, отдельно выделим наименьшие из них следующим образом:

Определение

Периодом $T(u)$ последовательности u называется наименьшее число $t \in \mathbb{N}$, для которого существует $\lambda \in \mathbb{Z}_+$ такое, что выполняется равенство (11.3), при этом *длиной подхода $\Lambda(u)$ последовательности u* называется наименьшее число $\lambda \in \mathbb{Z}_+$, для которого выполняется равенство

$$u(i + T(u)) = u(i)\ \forall i \geqslant \lambda. \tag{11.5}$$

Напоминание: Общие свойства и параметры периодических последовательностей.

Теорема

Пусть $u \in \Omega^{\infty}$ — периодическая последовательность. Числа $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$ удовлетворяют равенству (11.3) тогда и только тогда, когда

$$\lambda \geqslant \Lambda(u), \ \ T(u) | t.$$

Напоминание: Общие свойства и параметры периодических последовательностей.

Предложение

Пусть $u, v \in \mathcal{R}^{\infty}$ — периодические последовательности над кольцом $\mathcal{R}$. Тогда
1. сумма этих последовательностей $w = u + w$ также является периодической последовательностью и

$$\Lambda(w) \leqslant \max\{\Lambda(u), \Lambda(v)\}, \;\; T(w) | [T(u), T(v)]; \tag{11.6}$$

2. если $\Lambda(u) \neq \Lambda(v)$, то

$$\Lambda(w) = \max\{\Lambda(u), \Lambda(v)\}; \tag{11.7}$$

Общие свойства и параметры периодических последовательностей.

Предложение

3. если $(T(u), T(v)) = 1$, то

$$T(w) = [T(u), T(v)]; \tag{11.8}$$

4. если u и v — ЛРП, обладающие взаимно простыми характеристическими многочленами, то также выполнены равенства (11.7) и (11.8).

Напоминание: Специальные классы периодических последовательностей.

Определение

Периодическая последовательность u над кольцом $\mathcal{R}$ называется *чисто периодической*, или *реверсивной*, если $\Lambda(u) = 0$.

Определение

Периодическая последовательность u над кольцом $\mathcal{R}$ называется *вырождающейся*, если $u = (u(0), \ldots, u(\lambda - 1), 0, \ldots, 0, \ldots)$ для некоторого $\lambda \in \mathbb{N}$.

Специальные классы периодических последовательностей.

Очевидно следующее утверждение:

Предложение

1. $u \in \mathcal{R}^{\infty}$ — чисто периодическая последовательность тогда и только тогда, когда $u \in L_{\mathcal{R}}(x^t - 1)$ для некоторого $t \in \mathbb{N}$.
2. $u \in \mathcal{R}^{\infty}$ — вырождающаяся последовательность тогда и только тогда, когда $u \in L_{\mathcal{R}}(x^{\lambda})$ для некоторого $\lambda \in \mathbb{Z}_{+}$.
3. Одновременно чисто периодической и вырождающейся является только нулевая последовательность.

Специальные классы периодических последовательностей.

Теорема

Любая периодическая последовательность u над кольцом $\mathcal{R}$ однозначно представляется в виде суммы $u = u_0 + u_1$, где u_0 — вырождающаяся, u_1 — чисто периодическая последовательности. При этом

$$\Lambda(u) = \Lambda(u_0), \;\; T(u) = T(u_1). \tag{11.9}$$

Напоминание: Периодические многочлены. Периодичность ЛРП над конечным кольцом.

Пусть далее $\mathcal{R}$ — конечное коммутативное кольцо с $1 \neq 0$.

Определение

Многочлен $F(x) \in \mathcal{R}[x]$ назовём *периодическим*, если существуют индексы $\lambda \in \mathbb{Z}_+$, $t \in \mathbb{N}$ такие, что

$$F(x) | x^{\lambda}(x^t - 1). \tag{11.10}$$

Периодом $T(F)$ многочлена $F(x)$ называется наименьшее число $t \in \mathbb{N}$, для которого существует $\lambda \in \mathbb{Z}_+$ такое, что выполняется равенство (11.10), при этом *длиной подхода $\Lambda(F)$ многочлена $F(x)$* называется наименьшее число $\lambda \in \mathbb{Z}_+$, для которого выполняется равенство $F(x)|x^{\lambda}(x^{T(F)} - 1)$. Унитарный периодический многочлен $F(x)$ со свойством $\Lambda(F) = 0$ назовём *реверсивным*.

Напоминание: Периодические многочлены и последовательности.

Покажем связь периодических многочленов с периодическими последовательностями:

Предложение

1. Унитарный многочлен $F(x) \in \mathcal{R}[x]$ является периодическим тогда и только тогда, когда периодична ЛРП $e^F \in L_{\mathcal{R}}(F)$.
2. Если $F(x) \in \mathcal{R}[x]$ — периодический, то $\Lambda(F) = \Lambda(e^F)$, $T(F) = T(e^F)$.
3. Если $F(x) \in \mathcal{R}[x]$ — периодический, то любая ЛРП $u \in L_{\mathcal{R}}(F)$ есть периодическая последовательность, для которой $\Lambda(u) \leqslant \Lambda(F)$, $T(u) | T(F)$.

Напоминание: Периодичность ЛРП над конечным кольцом.

Теорема

Пусть $F(x) \in \mathcal{R}[x]$ — унитарный многочлен степени $m > 0$ над конечным кольцом $\mathcal{R}$. Тогда
1. $F(x)$ — периодический многочлен, причём если $|\mathcal{R}|^m > 2$, то

$$\Lambda(F) + T(F) \leqslant |\mathcal{R}|^m - 1;$$

2. $F(x)$ — реверсивный многочлен тогда и только тогда, когда $F(0) \in \mathcal{R}^*$;
3. произвольная ЛРП $u \in L_{\mathcal{R}}(F)$ является периодической последовательностью, причём если $|\mathcal{R}|^m > 2$, то $\Lambda(u) + T(u) \leqslant |\mathcal{R}|^m - 1$.

Периоды многочленов и ЛРП над полем.

Пусть $\mathbb{F} = GF(q)$, $q = p^n$, p — простое.
Период и длину подхода ЛРП над полем можно определить через её минимальный многочлен:

Предложение

Пусть u — ЛРП над полем $\mathbb{F}$. Тогда $\Lambda(u) = \Lambda(M_u(x))$, $T(u) = T(M_u(x))$.

◄ Следует из теоремы о минимальном многочлене ЛРП, поскольку

$$\forall \lambda \in \mathbb{Z}_+, t \in \mathbb{N}: \ x^\lambda(x^t - 1) \cdot u = (0) \Leftrightarrow M_u(x) | x^\lambda(x^t - 1).$$

►

В дальнейшем мы покажем, как вычислить период и длину подхода произвольного унитарного многочлена. Задача сводится к разложению его на неприводимые сомножители, и определению соответствующих параметров неприводимых многочленов.

Поле разложения и корни неприводимого многочлена над конечным полем.

Напомним, что *поле разложения $\mathbb{E}$ многочлена* $F(x) \in \mathbb{F}[x]$ — минимальное расширение $\mathbb{F}$, в котором $F(x)$ раскладывается на линейные множители. Заметим, что $\mathbb{E}$ как конечное расширение конечного поля само является конечным полем.

Теорема

Пусть $\mathbb{F} = GF(q)$, $q = p^n$, p — простое. Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m и $\mathbb{K} = \mathbb{F}(\alpha)$ — поле, порождённое некоторым (произвольным) корнем α многочлена $F(x)$. Тогда

1. $\mathbb{K} = \mathbb{E}$ — поле разложения многочлена $F(x)$, причём $F(x)$ имеет в $\mathbb{K}$ m различных корней

$$\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}};$$

2. $F(x) | x^{q^m} - x$.

Поле разложения и корни неприводимого многочлена над конечным полем.

◀ 1. Пусть $F(x) = \sum\limits_{i=0}^{m} f_i x^i$, $f_i \in \mathbb{F}$. По следствию из теооремы Лагранжа имеем $f_i^q = f_i$ для всех $i = 0, \dots, m$. Тогда для любого $s \in \mathbb{N}$ имеем

$$F(\alpha^{q^s}) = \\ = \sum_{i=0}^{m} f_i \cdot (\alpha^{q^s})^i = \sum_{i=0}^{m} f_i \cdot (\alpha^i)^{q^s} = \sum_{i=0}^{m} (f_i \alpha^i)^{q^s} = \left(\sum_{i=0}^{m} f_i \alpha^i \right)^{q^s} = \\ = (F(\alpha))^{q^s} = 0.$$

Поэтому все числа $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ являются корнями многочлена $F(x)$.
Докажем, что они различны.

Поле разложения и корни неприводимого многочлена над конечным полем.

Предположим противное: $\alpha^{q^s} = \alpha^{q^t}$ для $0 \leqslant s < t \leqslant m-1$. Тогда при $r = t - s$ получаем $0 = \alpha^{q^{s+r}} - \alpha^{q^s} = (\alpha^{q^r} - \alpha)^{q^s}$. Значит, $\alpha^{q^r} = \alpha$ для некоторого $0 < r < m$.

Элементы поля $\mathbb{K}$ имеют вид $\beta = \sum\limits_{i=0}^{m-1} c_i \alpha^i$, $c_i \in \mathbb{F}$. Поскольку $c_i^{q^r} = c_i$ для всех $i = 0, \ldots, m-1$, то из доказанному выше получаем $\beta^{q^r} = \beta$. Следовательно, все q^m элементов поля $\mathbb{K}$ являются корнями многочлена $x^{q^r} - x$, что невозможно, поскольку $r < m$. Противоречие.

2. Известно, что $|\mathbb{K}| = q^m$ и все элементы поля $\mathbb{K}$ являются корнями многочлена $G(x) = x^{q^m} - x \in \mathbb{F}[x]$. Значит, $F(x)$ и $G(x)$ не взаимно просты над полем $\mathbb{K}$, а тогда и над $\mathbb{F}$. Ввиду неприводимости многочлена $F(x)$ над полем $\mathbb{F}$ получаем, что $F(x) | G(x)$. ▶

Поле разложения и корни неприводимого многочлена над конечным полем.

Следствие

Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m, $F(x) \neq x$ и α, β — корни многочлена $F(x)$ в его поле разложения $\mathbb{E}$. Тогда в мультипликативной группе $\mathbb{E}^*$

1. $\operatorname{ord}\alpha = \operatorname{ord}\beta$;
2. $\operatorname{ord}\alpha | q^m - 1$;
3. $\operatorname{ord}\alpha \nmid q^r - 1$ для $0 < r < m$.

Поле разложения и корни неприводимого многочлена над конечным полем.

◀ 1. Пусть $\operatorname{ord}\alpha = d$. Тогда α — корень многочлена $x^d - 1 \in \mathbb{F}[x]$. Следовательно, $(F(x), x^d - 1) \neq 1$, поэтому $F(x) | x^d - 1$. Поскольку $F(\beta) = 0$, то $\operatorname{ord}\beta \leqslant d = \operatorname{ord}\alpha$. Аналогично, $\operatorname{ord}\alpha \leqslant \operatorname{ord}\beta$.
2. Согласно пункту 2 предыдущей теоремы $F(x)|x(x^{q^m-1} - 1)$. Ввиду неприводимости многочлена $F(x)$ и условия $F(x) \neq x$ получаем, что $F(x)|x^{q^m-1} - 1$. Откуда $\operatorname{ord}\alpha | q^m - 1$.
3. Следует из доказательства пункта 1 предыдущей теоремы.▶

НОК порядков корней.

Определение

Для многочлена $F(x) \in \mathbb{F}[x]$ определим параметр $O(F)$ как НОК порядков всех ненулевых корней многочлена $F(x)$ в мультипликативной группе его поля разложения над $\mathbb{F}$; положим $O(F) = 1$ для $F(x) = x^l$, $l \in \mathbb{N}$.

Вычисление периода неприводимого многочлена.

Теорема

Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m. Тогда
1. $\Lambda(F) = 0$, т.е. любой неприводимый многочлен над полем является реверсивным;
2. $T(F) = O(F)$;
3. $T(F) | q^m - 1$, в частности, $(T(F), p) = 1$, и $T(F) \nmid q^k - 1$ для $k \in \{1, \dots, m-1\}$.

Вычисление периода неприводимого многочлена.

◀ 1. В силу неприводимости $F(x)$ не делится на x, т.е. $F(0) \neq 0$, и реверсивность следует из пункта 2 теоремы о периодичности ЛРП.
2. Пусть $\mathbb{E}$ — поле разложения $F(x)$ над $\mathbb{F}$. Тогда порядки всех корней $F(x)$ в $\mathbb{E}$ одинаковы, поэтому $O(F) = \operatorname{ord}\alpha$ для произвольного корня $\alpha \in \mathbb{E}$.
Так как по определению $F(x)|x^{T(F)} - 1$, то $\alpha^{T(F)} = 1$, значит $O(F) = \operatorname{ord}\alpha | T(F)$.
Обратно, поскольку $\alpha^{O(F)} = 1$, то $(F(x), x^{O(F)} - 1) \neq 1$. Из неприводимости $F(x)$ тогда получаем, что $F(x)|x^{O(F)} - 1$, т.е. $T(F)|O(F)$. Следовательно, $T(F) = O(F)$.
3. Поскольку $\alpha \in \mathbb{E}^*$, то $\operatorname{ord}\alpha | |\mathbb{E}^*| = q^m - 1$. Значит, по пункту 2, $T(F)|q^m - 1$. Заметим, что если $T(F)|q^k - 1$ при $k < m$, то $\alpha^{q^k} = \alpha$, противоречие с тем, что $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ — это все различные корни многочлена $F(x)$. ▶

Алгоритм нахождения периода неприводимого многочлена

Пусть $F(x) \in \mathbb{F}[x]$ — неприводимый многочлен степени m.
Шаг 1. Находим все делители числа $q^m - 1$, не являющиеся делителями чисел $q-1, \ldots, q^{m-1}-1$ и далее осуществляем по ним перебор.
Шаг 2. Для каждого найденного на Шаге 1 числа t проверяем выполнение условия

$$x^t \equiv 1 \pmod{F(x)}.$$

Шаг 3. Наименьшее из таких t, для которых выполнено условие Шага 2, и есть период $T(F)$.

Вычисление периода произвольного многочлена над полем по его каноническому разложению.

Теорема

Пусть $F(x) \in \mathbb{F}[x]$ — унитарный многочлен, имеющий каноническое разложение

$$F(x) = x^l G_1(x)^{k_1} \cdots G_s(x)^{k_s}$$

на неприводимые множители. Положим

$$k = \max\{k_1, \ldots, k_s\}, \; c = \lceil \log_p k \rceil,$$

т.е. число $c \in \mathbb{Z}_+$ находится из условия $p^{c-1} < k \leqslant p^c$. Тогда

$$\Lambda(F) = l, \; T(F) = p^c O(F) = p^c [T(G_1), \ldots, T(G_s)].$$

Вычисление периода произвольного многочлена над полем по его каноническому разложению.

◀ Положим $H(x) = G_1(x)^{k_1} \cdots G_s(x)^{k_s}$. Согласно пункту 2 теоремы о перодичности ЛРП, многочлен $H(x)$ является реверсивным. По следствию для произведения многочленов имеем: $\Lambda(F) = \Lambda(x^l) = l$, $T(F) = T(H)$.
Пусть далее $G(x) = G_1(x) \cdots G_s(x)$. Очевидно, что $O(F) = O(G) = [O(G_1), \ldots, O(G_s)]$. Из теоремы 11.28 следует, что выполнено равенство $[O(G_1), \ldots, O(G_s)] = [T(G_1), \ldots, T(G_s)]$. В свою очередь, $[T(G_1), \ldots, T(G_s)] = T(G)$ согласно следствию для произведения многочленов. Остаётся доказать равенство $T(H) = p^c T(G)$.

Вычисление периода произвольного многочлена над полем по его каноническому разложению.

Поскольку $G(x)|x^{T(G)}-1$, то по определению параметров k и c отсюда следует, что $H(x)|(x^{T(G)}-1)^k$ и $H(x)|(x^{T(G)}-1)^{p^c}$. Над полем характеристики p верно равенство $(x^{T(G)}-1)^{p^c}=x^{T(G)p^c}-1$. Отсюда получаем, что $T(H)|T(G)p^c$. Более того, $T(G)|T(H)$ (поскольку $G(x)|H(x)$), следовательно, $T(H)=T(G)p^d$ для некоторого $d\leqslant c$. По пункту 3 теоремы 11.28 имеем $(T(G_i),p)=1$, $i=1,\ldots,s$. Значит, $(T(G),p)=1$. Отсюда следует, что многочлен $x^{T(G)}-1$ взаимно прост со своей производной, поэтому не имеет кратных множителей в каноническом разложении над $\mathbb{F}$. Тогда в каноническом разложении многочлена $x^{T(H)}-1=(x^{T(G)}-1)^{p^d}$ каждый неприводимый множитель имеет кратность p^d. С другой стороны, $H(x)|x^{T(H)}-1$, поэтому $k_i\leqslant p^d$, $i=1,\ldots,s$, и значит, $k\leqslant p^d$. По определению параметра c отсюда следует, что $c\leqslant d$. Таким образом, $d=c$, и $T(H)=T(G)p^c$. ▶

Существование и свойства ЛРП максимального периода над конечным полем.

Пусть u — ЛРП ранга m над полем $\mathbb{F}$. По теореме о периодичности ЛРП при условии $q^m > 2$ период и длина подхода последовательности u удовлетворяют неравенству $\Lambda(u) + T(u) \leqslant q^m - 1$. Интерес представляют последовательности, для которых эта оценка превращается в равенство, и более того, чтобы период был наибольшим, а именно:

Определение

Последовательность $u \in \mathbb{F}^\infty$ называется *ЛРП максимального периода над* $\mathbb{F}$, если для некоторого $m \in \mathbb{N}$ последовательность u есть ЛРП ранга m и периода $q^m - 1$.

Существование и свойства ЛРП максимального периода над конечным полем.

Очевидно, что для $q^m > 2$ при этом ЛРП u максимального периода над $\mathbb{F}$ есть чисто периодическая последовательность ($\Lambda(u) = 0$), соответственно, её минимальный многочлен реверсивен.
Заметим, что ЛРП u максимального периода $q^m - 1$ над полем $\mathbb{F} = GF(q)$ не будет ЛРП максимального периода над его расширением $\mathbb{K} = GF(q^t)$, $t > 1$, поскольку $T(u) \neq q^{tm} - 1$.

Существование и свойства ЛРП максимального периода над конечным полем даёт следующая теорема:

Теорема

Пусть u — ЛРП над полем $\mathbb{F} = GF(q)$ с реверсивным минимальным многочленом $M_u(x)$ степени m, причём $q^m > 2$. Тогда следующие утверждения эквивалентны:
1. u — ЛРП максимального периода над $\mathbb{F}$;
2. любая ненулевая ЛРП $v \in L_{\mathbb{F}}(M_u)$ есть сдвиг последовательности u, т.е. $v = x^k \cdot u$ для некоторого $k \in \mathbb{Z}_+$;
3. многочлен $M_u(x)$ неприводим над $\mathbb{F}$, и его корень α в поле разложения $\mathbb{E} = GF(q^m)$ над $\mathbb{F}$ есть примитивный элемент поля $\mathbb{E}$;
4. $T(M_u) = q^m - 1$.

Существование и свойства ЛРП максимального периода над конечным полем.

◀ "1) $\Rightarrow$ 2)" Так как $T(u) = q^m - 1$, то все последовательности $u, x \cdot u, \dots, x^{q^m-1} \cdot u$ различны и принадлежат $L_{\mathbb{F}}(M_u) \setminus \{(0)\}$. Поскольку по предложению о задании ЛРП начальным вектором $|L_{\mathbb{F}}(M_u) \setminus \{(0)\}| = q^m - 1$, то эти последовательности исчерпывают множество $L_{\mathbb{F}}(M_u) \setminus \{(0)\}$.

"2) $\Rightarrow$ 3)" По условию теоремы $(M_u(x), x) = 1$. Если любая ненулевая ЛРП $v \in L_{\mathbb{F}}(M_u)$ имеет вид $v = x^k \cdot u$, то по пункту 2 теоремы о минимальном многочлене получаем, что

$$M_v(x) = \frac{M_u(x)}{(M_u(x), x^k)} = M_u(x).$$

Тогда согласно следствию о минимальном многочлене, многочлен $M_u(x)$ неприводим над $\mathbb{F}$.

Как показано в доказательстве пункта 2 теоремы 11.28, $T(M_u) = O(M_u) = \operatorname{ord}\alpha$. Из условия, что

$$|\left\{x^k \cdot u | k \in \mathbb{Z}_+\right\}| = |L_{\mathbb{F}}(M_u) \setminus \{(0)\}| = q^m - 1$$

следует, что $T(u) = q^m - 1$. Из равенства $T(M_u) = T(u) = q^m - 1$ следует, что α является образующим элементом группы $(\mathbb{E}^*, \cdot)$, т.е. примитивным элементом поля $\mathbb{E}$.
"3) $\Rightarrow$ 4)" При условии 3, $\operatorname{ord}\alpha = q^m - 1$ и $O(M_u) = \operatorname{ord}\alpha$, тогда согласно пункту 2 теоремы 11.28 имеем $T(M_u) = \operatorname{ord}\alpha = q^m - 1$.
"4) $\Rightarrow$ 1)" очевидно. ▶

Многочлены максимального периода.

Теорема 11.31 показывает, что задача построения ЛРП максимального периода $q^m - 1$ над полем $\mathbb{F} = GF(q)$ сводится к построению реверсивного многочлена $F(x) \in \mathbb{F}[x]$, удовлетворяющего пункту 3 указанной теоремы.

Определение

Реверсивный многочлен $F(x) \in \mathbb{F}[x]$ называется *многочленом максимального периода*, или *примитивным* многочленом, над полем $\mathbb{F}$, если он имеет степень m и период $q^m - 1$.

Предложение

Число многочленов степени m максимального периода $q^m - 1$ над полем $\mathbb{F} = GF(q)$ равно $\dfrac{1}{m}\varphi(q^m - 1)$, где φ — функция Эйлера.

◀ Из теоремы 11.31 следует, что многочлен $F(x) \in \mathbb{F}[x]$ степени m максимального периода имеет в поле $\mathbb{E} = GF(q^m)$ в точности m корней, каждый из которых является примитивным элементом поля $\mathbb{E}$. Два различных унитарных неприводимых многочлена не могут иметь общий корень над $\mathbb{E}$, так как в этом случае они имели бы общий делитель положительной степени над $\mathbb{E}$, а значит, их НОД над $\mathbb{F}$ был бы положительной степени, что невозможно ввиду неприводимости. Число примитивных элементов вычисляется как число образующих циклической группы $(\mathbb{E}^*, \cdot)$ — оно равно $\varphi(q^m - 1)$. ▶

Многочлены максимального периода.

Следующее утверждение даёт критерий проверки того, что многочлен является многочленом максимального периода:

Предложение

Неприводимый многочлен $F(x) \in \mathbb{F}[x]$ степени $m > 0$ является многочленом максимального периода над полем $\mathbb{F}$ тогда и только тогда, когда $F(x) \neq x$, и для каждого собственного простого делителя d числа $q^m - 1$ выполняется условие

$$x^{\frac{q^m-1}{d}} \not\equiv 1 \pmod{F(x)}. \tag{11.11}$$

◀ Так как $F(x)$ неприводим над $\mathbb{F} = GF(q)$, то по теореме 11.28 $T(F)|q^m - 1$ и условие, что $T(F) < q^m - 1$ равносильно тому, что для некоторого собственного простого делителя d числа $q^m - 1$ выполняется условие делимости $T(F)|\dfrac{q^m-1}{d}$, т.е. не выполняется равенство (11.11). ▶

Алгоритм построения многочлена максимального периода

Выполняется перебор неприводимых многочленов степени m с проверкой равенства $T(F) = q^m - 1$ с помощью условия (11.11).

Следствие

Если $2^m - 1$ — простое число (это так называемые простые числа Мерсенна), то любой неприводимый многочлен над $GF(2)$ степени m есть многочлен максимального периода.