1. Линейные рекуррентные последовательности над конечным полем

{ Содержание раздела:

Характеристический, минимальный и аннулирующий многочлены, сопровождающая матрица.

Оценки минимального периода линейных рекуррентных последовательностей (ЛРП).

ЛРП максимального периода.

Суммирование и произведение рекуррентных последовательностей.

Представление ЛРП через функцию след.

}

В общем случае рекуррентная последовательность x(i), i=0,1,…, на заданном множестве A определяется соотношением

$$x(i+m)=f(x(i),x(i+1),\ldots,x(i+m-1)),\ i\geq 0,$$

где $f:A^m\rightarrow A$ – некоторая функция от m переменных.

Такая последовательность вырабатывается конечным автоматом, который называется регистром сдвига с функцией обратной связи f.

Наиболее глубоко изучены криптографические качества рекуррентных последовательностей для случая, когда множество A является конечным полем $A=P=F_q$, а функция f – линейна.

1.1. Определение. Последовательность u=u(0),u(1),… элементов поля P называется линейной рекуррентной последовательностью (ЛРП) порядка m>0 над полем P, если существуют константы $f_0,f_{1,\ldots},f_{m-1}\in P$ такие, что

$$u(i+m)=\sum_{j=0}^{m-1} f_j\cdot u(i+j),\ i\geq 0. \qquad (1.1)$$

ЛРП реализуется схемой линейного регистра сдвига. В очередном такте работы регистра сдвига содержащиеся в ячейках его накопителя значения умножаются на соответствующие коэффициенты f_j и суммируются (умножение и сложение проводится в поле P). После этого происходит сдвиг (влево) информации в регистре, а в освободившуюся крайнюю ячейку записывается вычисленное значение суммы (значение функции f обратной связи).

Равенство (1.1), выражающее зависимость между знаками ЛРП, называют законом рекурсии, многочлен $f(x)=x^m-\sum_{j=0}^{m-1} f_j\cdot x^j$ характеристическим многочленом ЛРП, вектор $u_0^{\rightarrow}=(u(0),u(1),\ldots,u(m-1))$

начальным состоянием (вектором) ЛРП, и соответственно вектор $u_t^{\rightarrow}=(u(t),u(t+1),\ldots,u(t+m-1))$ _ состоянием (вектором) ЛРП в такт t.

Векторы состояний ЛРП связаны соотношением

$$u_t^{\rightarrow}= u_0^{\rightarrow}\cdot A^t,\ t=0,1,\ldots, \qquad (1.2)$$

где квадратная (m×m) матрица A называется сопровождающей матрицей соответствующей ЛРП и имеет вид

$$A=\begin{pmatrix} 000\ldots0\,f(0) \\ 100\ldots0\,f(1) \\ 010\ldots0\,f(2) \\ \ldots\ldots\ldots\ldots\ldots \\ 000\ldots1\,f(m-1) \end{pmatrix},\ f(j)=f_j,\ j=0,1,\ldots,m-1.$$

1.2. Определение. Периодом последовательности u=u(0),u(1),… называется натуральное число t, для которого существует число $n_0>0$ такое, что для всех i≥0 справедливо равенство

$$u(n_0+i+t)=u(n_0+i).$$

Наименьший из всех периодов периодической последовательности называется ее минимальным периодом, а число n_0 называется предпериодом.

Отметим, что понятие периода играет весьма важную роль в оценке криптографических свойств соответствующих последовательностей.

1.2.1. Утверждение. Каждый период периодической последовательности делится на ее минимальный период.

Доказательство. Пусть r – произвольный период периодической последовательности s(i), i≥0, и пусть r_1 – ее минимальный период. Тогда $s(n+r)=s(n)$ для всех $n\ge n_0$, и $s(n+r_1)=s(n)$ для всех $n\ge n_1$ при соответствующем выборе n_0 и n_1.

Если r не делится на r_1, то $r=m\cdot r_1+t$, где $m\ge1$, $0<t<r_1$. Отсюда для всех $n\ge\max\{n_0,n_1\}$ получаем

$$s(n)=s(n+r)=s(n+ m\cdot r_1+t)=s(n+(m-1)r_1+t)=\ldots=s(n+t).$$

Следовательно, число $t<r_1$ также является периодом данной последовательности. Полученное противоречие и завершает доказательство.

1.2.2. Определение. Периодическая последовательность s(i), i≥0, с минимальным периодом r называется чисто периодической, если равенство $s(i+n)=s(n)$ выполняется для всех n=0,1,…

1.2.3. Утверждение. Каждая ЛРП u=u(0),u(1),… k-го порядка над полем F_q является периодической, и ее минимальный период r удовлетворяет неравенству

$$r\le q^k-1.$$

Доказательство. Если начальный вектор ЛРП – нулевой, то и все следующие за ним векторы состояний равны нулевому вектору. Следовательно, период такой ЛРП равен $r=1\le q^k-1$. Пусть теперь начальный вектор не является нулевым. Тогда для некоторых i, j, $0\le i<j\le q^k-1$, будет совпадение векторов-состояний в такты i и j: $u_i^{\rightarrow}=u_j^{\rightarrow}$. Отсюда для всех $n\ge i$ будет выполняться равенство: $u(n+j-i)=u(n)$. Значит, число $r=j-i\le q^k-1$ является периодом данной ЛРП. Доказательство завершено.

1.2.4. Задача. Показать, что верхняя оценка предыдущего утверждения для минимального периода достигается для ЛРП, заданной соотношением: $u(n+1)=g\cdot u(n)$, n=0,1,…, $u(0)\ne 0$, g – примитивный элемент поля F_q.

1.2.5. Задача. Показать, что минимальный период ЛРП первого порядка над полем F_q делит число q-1.

1.3. Утверждение. ЛРП u=u(0),u(1),… с характеристическим многочленом $f(x)=x^m-\sum_{j=0}^{m-1} f_j\cdot x^j \in F_q[x]$ является чисто периодической при любом начальном состоянии $u_0^{\rightarrow}=(u(0),u(1),\ldots,u(m-1))\in(F_q)^m$ в том и только том случае, если коэффициент f_0 отличен от нуля.

Доказательство. Пусть r – минимальный период ЛРП, $n_0\ge 1$ – ее предпериод. Тогда при $f_0\ne 0$ будем иметь равенство

$u(n_0-1+r)=(f_0)^{-1}\cdot(u(n_0+m-1+r)-f_{m-1}\cdot u(n_0+m-2+r)-\ldots-f_1\cdot u(n_0+r))=$

$=(f_0)^{-1}\cdot(u(n_0+m-1)-f_{m-1}\cdot u(n_0+m-2)-\ldots-f_1\cdot u(n_0))=u(n_0-1).$

Тем самым, пришли к противоречию с тем, что n_0 – предпериод.

Если же $f_0=0$, то ЛРП с начальным состоянием (1,0,0,…,0), очевидно будет иметь период r=1 и предпериод $n_0=1$. На этом доказательство закончено.

1.3.1. Замечание. Так как определитель сопровождающей матрицы ЛРП, заданной соотношением (1.1), равен $\det(A)=(-1)^{m-1}\cdot f_0$, то чистая периодичность ЛРП равносильна невырожденности сопровождающей матрицы. Отметим при этом, что множество всех невырожденных (m×m) матриц над полем F_q образуют конечную группу относительно операции матричного умножения, которая носит название общей линейной группы и обозначается $GL(m, F_q)$.

1.4. Утверждение. Минимальный период ЛРП, заданной соотношением (1.1), $f_0\ne 0$, является делителем порядка сопровождающей матрицы A, рассматриваемой как элемент группы $GL(m, F_q)$.

Доказательство. Пусть ord(A)=k. Тогда из (1.2) получим

$$u_{n+k}^{\rightarrow}=u_0^{\rightarrow}A^{n+k}=u_0^{\rightarrow}A^n=u_n^{\rightarrow},\ n\ge 0.$$

Следовательно, k является периодом ЛРП. С учетом утверждения 1.2.1 на этом доказательство закончено.

Следующее утверждение описывает случай, когда минимальный период ЛРП совпадает с порядком сопровождающей матрицы.

1.4.1. Утверждение. Пусть векторы состояний $u_0^{\rightarrow}$, $u_1^{\rightarrow}$,…, $u_{m-1}^{\rightarrow}$, ЛРП с характеристическим многочленом $f(x)=x^m-\sum_{j=0}^{m-1} f_j \cdot x^j \in F_q[x]$, $f_0 \neq 0$, являются линейно независимыми над полем F_q. Тогда минимальный период ЛРП совпадает с порядком сопровождающей матрицы в группе $GL(m, F_q)$.

Доказательство. Пусть r – минимальный период ЛРП. Тогда с учетом (1.2) имеем соотношения

$$u_0^{\rightarrow}= u_0^{\rightarrow}A^r,\ u_1^{\rightarrow}= u_1^{\rightarrow}A^r,\ \ldots,\ u_{m-1}^{\rightarrow}= u_{m-1}^{\rightarrow}A^r,$$

или в матричной форме

$$U=U \cdot A^r,$$

где строки матрицы U образованы векторами $u_0^{\rightarrow}$, $u_1^{\rightarrow}$,…, $u_{m-1}^{\rightarrow}$. В силу невырожденности матрицы U отсюда вытекает, что $A^r=E$, где E – единичная матрица (единица группы $GL(m, F_q)$).

1.4.2. Следствие. Минимальный период ЛРП с характеристическим многочленом $f(x)=x^m-\sum_{j=0}^{m-1} f_j \cdot x^j \in F_q[x]$, $f_0 \neq 0$, и начальным состоянием $u_0^{\rightarrow}=(0,0,\ldots,0,1)$ равен порядку сопровождающей матрицы A в группе $GL(m,F_q)$.

Справедливость следствия непосредственно вытекает из утверждения 1.4.1 в силу линейной независимости векторов $u_0^{\rightarrow}A^j$, j=0,1,…,m-1.

1.5. Определение. Многочлен $h(x)=h_0+h_1x+\ldots+h_sx^s \in F_q[x]$ называется аннулирующим для последовательности u=u(0),u(1),… элементов поля F_q, если $\sum_{j=0}^{s} h_j \cdot u(n+j)=0$ для всех n=0,1,…

Отметим, что характеристический многочлен ЛРП является аннулирующим для данной последовательности. И обратно, нормированный аннулирующий многочлен, очевидно, является характеристическим.

1.5.1. Задача. Показать, что множество аннулирующих многочленов заданной последовательности элементов поля F_q является идеалом кольца $F_q[x]$.

Любая ЛРП, очевидно, обладает множеством различных рекуррентных соотношений типа (1.1). В этой связи вводится следующее определение.

1.6. Определение. Характеристический многочлен ЛРП u=u(0),u(1),…, имеющий наименьшую степень, называется ее минимальным многочленом, а степень минимального многочлена – линейной сложностью данной последовательности.

Таким образом, линейная сложность последовательности u=u(0),u(1),… определяет минимальную длину линейного регистра сдвига, реализующего данную последовательность.

1.6.1. Замечание. Минимальный многочлен нулевой последовательности полагается равным m(x)=1.

1.6.2. Утверждение. Любой характеристический многочлен ЛРП кратен минимальному многочлену.

Доказательство. Предположим, что характеристический многочлен f(x) не делится без остатка на минимальный многочлен m(x). Тогда в результате деления с остатком получим

$$f(x)=d(x)m(x)+r(x),\ \deg(r(x))<\deg(m(x)).$$

Следовательно (см. задачу 1.5.1), многочлен r(x)=f(x)-d(x)m(x) является аннулирующим для данной ЛРП. Значит, после своей нормировки (при которой степень многочлена сохраняется) многочлен r(x) становится характеристическим многочленом рассматриваемой ЛРП. Это противоречит тому, что многочлен m(x) является минимальным.

1.6.3. Следствие. Пусть над полем F_q задана ЛРП с характеристическим многочленом f(x), f(0)≠0. Если многочлен f(x) – неприводим над полем F_q, тогда минимальный многочлен данной ЛРП совпадает с f(x).

1.6.4. Теорема. Пусть $m(x)\in F_q[x]$, m(0)≠0, – минимальный многочлен ЛРП u=u(0),u(1),… над полем F_q. Тогда минимальный период ЛРП равен периоду ω(m) многочлена m(x).

Доказательство. Пусть r – минимальный период ЛРП. Тогда многочлен $f(x)=x^r-1$ является характеристическим многочленом для данной ЛРП, и с учетом утверждения 1.6.1 имеем

$$x^r-1=0 \pmod{m(x)}.$$

Отсюда следует, что r кратно периоду ω(m) многочлена m(x). С другой стороны, из равенства $x^{\omega(m)}-1=0 \pmod{m(x)}$ следует, что ω(m) является периодом ЛРП, т.е. ω(m) кратно r. На этом доказательство завершено.

Отсюда получаем следующее утверждение.

1.6.5. Следствие. Пусть над полем F_q задана ЛРП с неприводимым характеристическим многочленом f(x), f(0)≠0, deg(f(x))=m. Тогда минимальный период r данной ЛРП является делителем числа q^m-1.

1.6.6. Определение. Если минимальный период ЛРП над полем F_q с ненулевым начальным состоянием и неприводимым характеристическим многочленом f(x), f(0)≠0, deg(f(x))=m, равен q^m-1, то линейная рекуррентная последовательность называется ЛРП максимального периода.

1.6.7. Следствие. ЛРП над полем F_q обладает максимальным периодом в том и только том случае, когда ее характеристический многочлен примитивен.

1.7. **Теорема.** Пусть $f(x)= x^m-\sum_{j=0}^{m-1} f_j \cdot x^j \in F_q[x]$, $f_0\neq 0$, - характеристический многочлен ЛРП с начальным состоянием $u_0^{\rightarrow}$. Тогда минимальный многочлен m(x) данной ЛРП совпадает с f(x) в том и только том случае, если векторы состояний $u_0^{\rightarrow}, u_1^{\rightarrow},\ldots, u_{m-1}^{\rightarrow}$ линейно независимы.

Доказательство. Пусть для некоторого t вектор $u_t^{\rightarrow}$ есть линейная комбинация векторов $u_0^{\rightarrow}, u_1^{\rightarrow},\ldots, u_{t-1}^{\rightarrow}$:

$$u_t^{\rightarrow}=d_0 \cdot u_0^{\rightarrow}+d_1 \cdot u_1^{\rightarrow}+\ldots+ d_{t-1} \cdot u_{t-1}^{\rightarrow},\ d_j\in F_q. \qquad (1.3)$$

Умножая обе части данного равенства на A^n, где A – сопровождающая матрица, и учитывая соотношение (1.2), получим равенство

$$u_{t+n}^{\rightarrow}=d_0 \cdot u_n^{\rightarrow}+d_1 \cdot u_{n+1}^{\rightarrow}+\ldots+ d_{t-1} \cdot u_{n+t-1}^{\rightarrow},\ n\geq 0,$$

которое свидетельствует, что многочлен $d(x)=x^t-d_{t-1}x^{t-1} -\ldots-d_1x-d_0$ является характеристическим для рассматриваемой ЛРП.

Значит, при линейной независимости векторов $u_0^{\rightarrow}, u_1^{\rightarrow},\ldots, u_{m-1}^{\rightarrow}$ степень любого характеристического многочлена не может быть меньше, чем m. С учетом утверждения 1.6.2 отсюда следует, что m(x)=f(x). Тем самым, в одну сторону теорема доказана.

Пусть теперь m(x)=f(x). Предположим, что $u_0^{\rightarrow}, u_1^{\rightarrow},\ldots, u_{m-1}^{\rightarrow}$ являются линейно зависимыми. Тогда для некоторого $t\leq m-1$ будет выполнено соотношение вида (1.3), из которого следует, что многочлен

$$d(x)=x^t-d_{t-1}x^{t-1} -\ldots-d_1x-d_0,$$

степень которого не превосходит m-1, является характеристическим для рассматриваемой ЛРП. Отсюда $m=\deg(m(x))\leq\deg(d(x))\leq m-1$. Полученное противоречие и завершает доказательство.

1.7.1. **Следствие.** Пусть задана ЛРП с характеристическим многочленом $f(x)=x^m-\sum_{j=0}^{m-1} f_j \cdot x^j \in F_q[x]$, $f_0\neq 0$, и начальным состоянием $u_0^{\rightarrow}=(0,0,\ldots,0,1)$. Тогда ее минимальный многочлен совпадает с f(x).

1.7.2. **Замечание.** Из доказательства теоремы 1.7 следует, что минимальным многочленом соответствующей ЛРП является многочлен

$$d(x)=x^t-d_{t-1}x^{t-1} -\ldots-d_1x-d_0,$$

определяемый соотношением (1.3) при минимальном натуральном t.

2. Суммирование и перемножение линейных рекуррентных последовательностей

Для заданного нормированного многочлена $f(x)\in F_q[x]$, $f(0)\neq 0$, положительной степени через S(f) обозначим множество всех ЛРП u=u(0),u(1),… с характеристическим многочленом f(x). Так как при заданном характеристическом многочлене ЛРП однозначно определяется начальным состоянием, то $|S(f)|=q^m$, где $m=\deg(f(x))$.

Множество S(f) можно рассматривать как векторное пространство с естественными операциями покоординатного (почленного) сложения и умножения на элемент поля F_q.

2.1. Теорема. Пусть d(x) – произвольный нормированный делитель многочлена f(x). Тогда в множестве S(f) существует ЛРП, минимальный многочлен которой равен d(x).

Доказательство. Так как множество аннулирующих многочленов заданной ЛРП над полем F_q является идеалом кольца $F_q[x]$, имеет место включение: $S(d) \subseteq S(f)$. Теперь справедливость теоремы вытекает из того, что в множестве S(d) (в силу следствия 1.7.1) имеется ЛРП, минимальный многочлен которой равен d(x).

2.2. Теорема. Пусть f(x) и g(x) – два нормированных многочлена над полем F_q, не являющиеся постоянными многочленами. Тогда S(f) является подмножеством множества S(g) тогда и только тогда, когда f(x) делит g(x).

· Пусть $S(f) \subseteq S(g)$. Возьмем в S(f) импульсную функцию, для которой минимальный многочлен совпадает с f(x). В таком случае многочлен g будет делиться на f. Пусть теперь f(x) делит g(x). Тогда минимальный многочлен любой ЛРП из S(f) будет делителем g(x). Следовательно, любая такая ЛРП лежит в S(g). ·

2.3. Теорема. Пусть $f_1,f_2,\ldots,f_h$ – нормированные многочлены над полем F_q. Если эти многочлены взаимно просты, то пересечение

$$S(f_1)\cap\ldots\cap S(f_h)$$

содержит только нулевую последовательность. Если d(x) – нормированный многочлен, deg d(x) >0, являющийся наибольшим общим делителем многочленов $f_1,f_2,\ldots,f_h$, тогда

$$S(f_1)\cap\ldots\cap S(f_h) = S(d).$$

· Минимальный многочлен m(x) любой последовательности, лежащей в пересечении, должен быть делителем каждого многочлена $f_1,f_2,\ldots,f_h$. Если эти многочлены взаимно просты, тогда m(x)=1. Значит, пересечение состоит только из нулевой последовательности. Во втором случае многочлен m(x) будет делителем многочлена d(x). Отсюда

$$S(f_1)\cap\ldots\cap S(f_h) \subseteq S(d).$$

В другую сторону включение вытекает из теоремы 2.2. ·

2.4. Теорема. Пусть $f_1,f_2,\ldots,f_t$ – нормированные многочлены над полем F_q, $c(x)=НОК\{f_1,\ldots,f_t\}$. Тогда

$$S(f_1)+S(f_2)+\ldots+S(f_t)=S(c).$$

· Проведем доказательство для случая t=2. Пусть $V_1=S(f_1)$, $V_2=S(f_2)$, $d=НОД(f_1,f_2)$. Тогда

$\mathrm{Dim}\,(V_1+V_2)= \mathrm{Dim}\,(V_1)+ \mathrm{Dim}\,(V_2) - \mathrm{Dim}\,(V_1\cap V_2) =\deg(f_1)+\deg(f_2)-\deg(d)$.

Учитывая, что $c(x)=f_1 \cdot f_2/d$, получаем, что

$$\mathrm{Dim}\,(V_1+V_2)=\deg(c(x))=\dim(S(c(x))).$$

Таким образом, линейное пространство $S(f_1)+S(f_2)$ лежит в пространстве $S(c)$ и имеет равную с ним размерность. Значит, $S(f_1)+S(f_2)=S(c)$. ·

В частном случае, когда многочлены f и g являются взаимно простыми, тогда

$$S(f)+S(g)=S(fg).$$

А так как при этом пересечение $S(f)$ и $S(g)$ содержит только нулевую последовательность, то любую последовательность $\sigma \in S(fg)$ можно единственным образом представить суммой

$$\sigma=\sigma_1+\sigma_2,\ \sigma_1 \in S(f),\ \sigma_2 \in S(g).$$

2.5. Теорема (без доказательства)**.** Пусть m_i – минимальный многочлен ЛРП σ_i над полем F_q, i=1,2,…,t, r_i – ее минимальный период.

Если многочлены m_i попарно взаимно просты, тогда минимальный многочлен m суммы $\sigma=\sigma_1+\sigma_2+\ldots+\sigma_t$ равен произведению $m=m_1 \cdot m_2 \cdot \ldots \cdot m_t$, а минимальный период равен $r=НОК(r_1,\ldots,r_t)$.

2.6. Теорема (без доказательства)**.** Пусть σ_i – периодические последовательности над полем F_q, r_i – их минимальные периоды, i=1,2,…,t. Если числа r_i попарно взаимно просты, то минимальный период суммы $\sigma_1+\ldots+\sigma_t$ равен произведению $r_1 \cdot r_2 \cdot \ldots \cdot r_t$.

Рассмотрим итоговое множество возможных длин периодов последовательностей из семейства $S(f)$, $f(0)\neq 0$.

1 случай (f – неприводимый многочлен, deg (f)=m).

В этом случае период любой ненулевой последовательности из $S(f)$ будет равен $\omega=q^m-1$.

2 случай ($f = g^n$, g – неприводимый многочлен, deg (g)=m, n>1).

В этом случае период ненулевой последовательности из $S(f)$ будет лежать в множестве

$$\{e,\ p \cdot e, p^2 \cdot e,\ldots,p^t \cdot e\},$$

здесь

e – период многочлена g,

p – характеристика поля F_q,

t – наименьшее натуральное число, при котором $p^t \geq n$.

3 случай ($f=g_1^{n(1)} \cdot g_2^{n(2)} \cdot \ldots \cdot g_s^{n(s)}$, g_j – различные неприводимые многочлены).

В данном случае любая последовательность $\sigma \in S(f)$ единственным образом представляется суммой

$$\sigma=\sigma_1+\ldots+\sigma_s,\ \sigma_j \in S(g_j^{n(j)}).$$

При этом длины периодов r_j последовательностей σ_j исследованы случаем 2, а их минимальные многочлены взаимно просты. Следовательно, периоды результирующих последовательностей задаются множеством величин $НОК\{r_1,r_2,\ldots,r_s\}$.

Что касается перемножения последовательностей, то имеет место следующий важный результат.

2.7. Теорема. Пусть $f_1,\ldots,f_t$ – нормированные многочлены над полем F_q. Тогда существует многочлен $g(x)\in F_q[x]$, при котором

$$S(f_1)\cdot S(f_2)\cdot\ldots\cdot S(f_t) = S(g).$$

Следующая теорема показывает о возможности выражения элементов ЛРП через функцию след.

2.8. Теорема. Пусть характеристический многочлен $f(x)=x^m-\sum_{j=0}^{m-1} f_j\cdot x^j$ ЛРП $u=u(0),u(1),\ldots$ является неприводимым над полем $P=F_q$, θ - корень многочлена $f(x)$ в поле $Q=GF(q^m)$. Тогда существует единственная константа $a\in Q$, что

$$u(j)=tr_{Q/P}(a\cdot\theta^j),\ j\geq 0. \qquad (2.1)$$

Доказательство. Покажем, что при любом фиксированном $a\in Q$ последовательность (2.1) является ЛРП с характеристическим многочленом $f(x)$. Это вытекает из следующих равенств

$$\sum_{j=0}^{m-1} f_j\cdot u(i+j)=\sum_{j=0}^{m-1} f_j\cdot tr_{Q/P}(a\cdot\theta^{j+i})=tr_{Q/P}(a\cdot\theta^i\cdot\sum_{j=0}^{m-1} f_j\cdot\theta^j)=tr_{Q/P}(a\cdot\theta^i\cdot\theta^m)=u(i+m).$$

Так как число всех ЛРП с заданным характеристическим многочленом $f(x)$ равно q^m и совпадает с числом всех констант из поля Q, то для доказательства теоремы достаточно показать, что разные константы $a\in Q$ приводят к разным ЛРП.

Предположим, что для $a_1\neq a_2$ выполняется равенство

$$Tr_{Q/P}(a_1\cdot\theta^j)=tr_{Q/P}(a_2\cdot\theta^j),\ j\geq 0.$$

Тогда при $a=a_1-a_2\neq 0$ будет выполнено соотношение

$$Tr_{Q/P}(a\cdot\theta^j)=0,\ j\geq 0.$$

Учитывая, что элементы $1,\theta,\theta^2,\ldots,\theta^{m-1}$ образуют базис поля Q, рассматриваемого как векторное пространство над полем $P=F_q$, из линейности функции след вытекает, что уравнение $tr_{Q/P}(a\cdot x)=0$ имеет q^m решений в поле Q. Это противоречие завершает доказательство.

Любая периодическая последовательность может рассматриваться как ЛРП. Следовательно, для нее существует линейный регистр сдвига, который ее вырабатывает. Поэтому линейная сложность может рассматриваться как характеристика аналитической сложности псевдослучайной последовательности. Известно, что при случайном выборе последовательности периода t ее линейная сложность близка к $\frac{1}{2}t$.

Отметим также, что существуют эффективные алгоритмы нахождения линейной сложности заданной последовательности элементов конечного поля (например, алгоритм Берлекэмпа-Месси).

Литература

1. А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин, А.В.Черемушкин. Основы криптографии (учебное пособие). – М.: Гелиос АРВ, 2001. – 480 с.
2. Р. Лидл, Г. Нидеррайтер. Конечные поля (в 2-х томах). М., «Мир», 1988.
3. М.И. Рожков. Алгебра. Основы теории конечных групп, колец, полей. Учебное пособие. М., МГИЭМ, 2009. – 82 с.
4. Golomb S. W. Shift Register Sequences. San Francisco: Holden-Day, 1967.

6. Вопросы для самостоятельного рассмотрения

Задачи по теории линейных рекуррентных последовательностей

1. Найти минимальный многочлен m(x) для ЛРП 5-го порядка с х.м. $f(x)=x^5+x^2+1 \in F_2[x]$ и вектором начального состояния (00001).
2. Верно ли, что существует ЛРП с х.м. $f(x)=x^4+x^2+1 \in F_2[x]$, минимальный многочлен которой равен $m(x)=x^2+x+1$?

3. Найти первые три бита (нумерация координат слева направо) вектора 56 –го состояния ЛРП с х.м. $f(x)=(x^3+x+1)^5 \in F_2[x]$ и вектором начального состояния $(101100\ldots0) \in (F_2)^{15}$.
4. Верно ли, что в семействе S(f) ЛРП с х.м. $f(x)=(x^2+x+1)^8 \in F_2[x]$ существует ЛРП с минимальным периодом, равным 8?
5. Найти первые три бита (нумерация координат слева направо) вектора 57–го состояния ЛРП с х.м. $f(x)=(x^3+x^2+1)^4 \in F_2[x]$ и вектором начального состояния $(01100\ldots0) \in (F_2)^{12}$.
6. Найти минимальный многочлен m(x) для ЛРП 5-го порядка с х.м. $f(x)=x^5+x^4+1 \in F_2[x]$ и вектором начального состояния (00001).
7. Найти минимальный многочлен m(x) для ЛРП 5-го порядка с х.м. $f(x)=x^5+x+1 \in F_2[x]$ и вектором начального состояния (00001).
8. Верно ли, что в семействе S(f) ЛРП с х.м. $f(x)=(x+1)^{10} \in F_2[x]$ существует ЛРП с минимальным периодом, равным 4?
9. Найти первые три бита (нумерация координат слева направо) вектора 30–го состояния ЛРП с х.м. $f(x)=(x^3+x+1)^2 \in F_2[x]$ и вектором начального состояния $(111000) \in (F_2)^6$.
10. Найти минимальный период суммы двух ЛРП с х.м. $f_1(x)=x^3+x^2+1 \in F_2[x]$ и $f_2(x)=x^2+x+1 \in F_2[x]$ при условии, что начальный вектор каждой ЛРП отличен от нуля.
11. Найти минимальный многочлен m(x) для ЛРП 5-го порядка с х.м. $f(x)=x^5+x^3+1 \in F_2[x]$ и вектором начального состояния (00001).
12. Найти первые три бита (нумерация координат слева направо) вектора 50–го состояния ЛРП с х.м. $f(x)=(x^2+x+1)^{10} \in F_2[x]$ и вектором начального состояния $(001110\ldots0) \in (F_2)^{20}$.
12. Верно ли, что в семействе S(f) ЛРП с х.м. $f(x)=(x+1)^{10} \in F_2[x]$ существует ЛРП с минимальным периодом, равным 20?
13. Найти минимальный многочлен m(x) для ЛРП 3-го порядка с х.м. $f(x)=x^3+1 \in F_2[x]$ и вектором начального состояния (101).
14. Найти первые три бита (нумерация координат слева направо) вектора 56–го состояния ЛРП с х.м. $f(x)=(x^3+x+1)^5 \in F_2[x]$ и вектором начального состояния $(101100\ldots0) \in (F_2)^{15}$.
15. Найти минимальный период ЛРП с х.м. $f(x)=x^5+x^2+1 \in F_2[x]$ и вектором начального состояния (10110).
16. Найти минимальный период ЛРП с х.м. $f(x)=x^5+x^3+1 \in F_2[x]$ и вектором начального состояния (11100).
17. Верно ли, что в семействе S(f) ЛРП с х.м. $f(x)=(x^2+x+1)^8 \in F_2[x]$ существует ЛРП с минимальным периодом, равным 8?
18. Найти первые три бита (нумерация координат слева направо) вектора 57–го состояния ЛРП с х.м. $f(x)=(x^3+x^2+1)^4 \in F_2[x]$ и вектором начального состояния $(01100\ldots0) \in (F_2)^{12}$.
19. Найти минимальный многочлен m(x) для ЛРП 3-го порядка с х.м. $f(x)=x^3+1 \in F_2[x]$ и вектором начального состояния (111).