Math-Net.Ru

Общероссийский математический портал

А. Б. Шишков, Экспоненциальные выборки из линейных рекуррентных последовательностей, *Дискрет. матем.*, 2002, том 14, выпуск 3, 70–77

DOI: <https://doi.org/10.4213/dm255>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.60.19

26 апреля 2023 г., 12:59:28

Экспоненциальные выборки из линейных рекуррентных последовательностей

© 2002 г. А. Б. Шишков

Описаны минимальные многочлены выборок из геометрических прогрессий и линейных рекуррент максимального периода над конечным полем характеристики 2, для которых шаг выборки экспоненциально зависит от номера такта.

Как известно (см. [1]), линейная рекуррентная последовательность максимального периода $u(i)$ над полем $GF(2)$ может быть представлена с помощью функции след

$$u(i) = \text{tr}_2^{2^n}(c\theta^i), \quad i = 0, 1, \dots,$$

где c — некоторый ненулевой элемент, а θ — примитивный элемент поля $GF(2^n)$.

Напомним, что функция след из поля $GF(2^n)$ в поле $GF(2)$ определяется следующим образом:

$$\text{tr}_2^{2^n}(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}, \quad \alpha \in GF(2^n).$$

Ниже описываются минимальные многочлены и периоды последовательностей w и v вида

$$w(i) = \theta^{d^i}, \quad i = 0, 1, \dots, \quad (1)$$

$$v(i) = \text{tr}_2^{2^n}(\gamma\theta^{d^i}), \quad i = 0, 1, \dots, \quad (2)$$

где d — некоторое натуральное число, а γ — ненулевой элемент поля $GF(2^n)$.

Указанные последовательности могут рассматриваться как выборки из геометрической прогрессии над полем $GF(2^n)$ и линейной рекурренты максимального периода над $GF(2)$, соответственно, величина шага которых вычисляется как экспоненциальная функция от номера такта.

Теорема 1. Пусть $2^n - 1$ — простое число, а d — натуральное число, соответствующее примитивному элементу поля $GF(2^n - 1)$. Тогда минимальный многочлен $m_w(x)$ последовательности w равен $x^{2^n-2} - 1$.

Доказательство. Поскольку период последовательности с общим членом d^i равен $2^n - 2$, период w делит это число ($w \mid 2^n - 2$), а следовательно, выполняется соотношение

$$m_w(x) \mid x^{2^n-2} - 1.$$

Покажем, что степень $m_w(x)$ не может быть меньше $2^n - 2$, тогда утверждение теоремы будет доказано.

Предположим противное, то есть пусть

$$\deg m_w(x) = k < 2^n - 2.$$

Пусть при этом

$$m_w(x) = \sum_{t=0}^k c_t x^t.$$

Тогда для любого неотрицательного i выполняется соотношение

$$0 = \sum_{t=0}^k c_t w(i+t) = \sum_{t=0}^k c_t \theta^{d^{i+t}} = \sum_{t=0}^k c_t (\theta^{d^i})^{d^t}. \quad (3)$$

Это означает, что поскольку θ^{d^i} пробегает все ненулевые элементы поля $GF(2^n)$ за исключением единицы, корнями многочлена

$$C(x) = \sum_{t=0}^k c_t x^{d^t}$$

являются все элементы поля $GF(2^n)$ за исключением, быть может, единицы. Рассмотрим теперь многочлен $\bar{C}(x)$, получаемый приведением многочлена $C(x)$ по модулю $x^{2^n-1} - 1$. Очевидно, что все ненулевые элементы поля $GF(2^n)$, являющиеся корнями $C(x)$, будут в свою очередь и корнями $\bar{C}(x)$. Следовательно, корнями $\bar{C}(x)$ будут все ненулевые элементы поля $GF(2^n)$, за исключением, быть может, единицы. Покажем, что нуль также является корнем $\bar{C}(x)$. Действительно, легко проверяется справедливость равенства

$$\bar{C}(x) = \sum_{t=0}^k c_t x^{d^t \bmod (2^n-1)}.$$

Нетрудно видеть, что ни для какого t число d^t не может делиться на $2^n - 1$, поэтому все члены многочлена $\bar{C}(x)$ имеют степень, большую нуля, следовательно, нуль — корень $\bar{C}(x)$. Кроме того, поскольку d — примитивный элемент поля $GF(2^n - 1)$ и $k < 2^n - 2$, в последней сумме нет членов с одинаковыми степенями, а значит, $\bar{C}(x)$ не может быть нулевым многочленом. Таким образом, этот многочлен имеет не менее $2^n - 1$ корней в поле $GF(2^n)$, однако степень его не выше $2^n - 2$. Получено противоречие с тем, что $k < 2^n - 2$. Таким образом, теорема доказана.

Следствие 1. Период последовательности w равен $2^n - 2$ и совпадает с ее рангом.

Для доказательства следующей ниже теоремы о строении минимального многочлена последовательности v вида (2) нам потребуются некоторые факты, касающиеся свойств так называемых линеаризованных многочленов, которые мы, следуя [1], приводим ниже.

Многочлен вида

$$L(x) = \sum_{i=0}^t \alpha_i x^{q^i}$$

с коэффициентами из некоторого расширения $GF(q^m)$ поля $GF(q)$ называется q -многочленом над $GF(q^m)$ (в нашем случае m будет всегда равно единице). Если число q фиксировано, то $L(x)$ принято также называть линейризованным многочленом. Для q -многочленов $L_1(x)$, $L_2(x)$ определяется операция символического умножения следующим образом:

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

Если рассматриваются лишь многочлены над $GF(q)$, то легко проверяется, что символическое умножение коммутативно, ассоциативно и дистрибутивно относительно обычного сложения. Операция символического умножения связана с обычной арифметикой многочленов с помощью следующего понятия. Многочлены

$$l(x) = \sum_{i=0}^t \alpha_i x^i, \quad L(x) = \sum_{i=0}^t \alpha_i x^{q^i}$$

над полем $GF(q^m)$ называются q -ассоциированными друг с другом. При этом $l(x)$ называется просто q -ассоциированным с $L(x)$ многочленом, а $L(x)$ — линейризованным q -ассоциированным с $l(x)$ многочленом. Справедлива следующая теорема.

Теорема 2 ([1], с. 149). Пусть q -ассоциированными с q -многочленами $L_1(x)$ и $L_2(x)$ являются многочлены $l_1(x)$ и $l_2(x)$ соответственно. Тогда следующие свойства эквивалентны:

- многочлен $L_1(x)$ символически делит многочлен $L_2(x)$;
- многочлен $L_1(x)$ делит $L_2(x)$ в обычном смысле;
- многочлен $l_1(x)$ делит многочлен $l_2(x)$.

Пусть $L(x)$ — ненулевой q -многочлен над полем $GF(q^m)$. Корень ζ этого многочлена называется q -первообразным корнем над $GF(q^m)$, если он не является корнем никакого ненулевого q -многочлена над $GF(q^m)$ более низкой степени. Однозначно определяемый унитарный линейризованный многочлен $L(x)$ наименьшей возможной степени, для которого ζ является q -первообразным корнем над $GF(q^m)$, называется минимальным q -многочленом элемента ζ над $GF(q^m)$. Справедлива также следующая теорема.

Теорема 3 ([1], с. 155). Элемент ζ является корнем q -многочлена $K(x)$ над полем $GF(q)$ тогда и только тогда, когда его минимальный q -многочлен $L(x)$ символически делит $K(x)$.

Пусть теперь ζ — ненулевой элемент поля $GF(q^n)$. Поскольку в этом случае ζ является корнем многочлена

$$F(x) = x^{q^n} - x,$$

то по теореме 3 его минимальный q -многочлен $L(x)$ делит $F(x)$ и, следовательно, по теореме 2, q -ассоциированный с $L(x)$ многочлен $l(x)$ делит многочлен $x^n - 1$.

Докажем теперь теорему, описывающую минимальный многочлен последовательности v вида (2).

Теорема 4. Пусть последовательность v имеет вид (2), $2^n - 1$ — простое число, а d — примитивный элемент поля $GF(2^n - 1)$. Пусть $L(x)$ — минимальный 2-многочлен элемента γ над $GF(2)$, а $l(x)$ — 2-ассоциированный с $L(x)$ многочлен. Справедливы следующие утверждения.

- (1) Если $\deg l(x) = n$, то минимальный многочлен $m_v(x)$ последовательности v имеет вид

$$m_v(x) = x^{2^n-2} - 1.$$

- (2) Если $\deg l(x) = 1$ (то есть, $\gamma = 1$), то

$$m_v(x) = x^{(2^n-2)/n} - 1.$$

- (3) Если $1 < \deg l(x) < n$, то степень $m_v(x)$ не меньше $(2^n - 2)/n$, а если выполняется условие

$$n - 1 = \min(a: 2^a \equiv 1 \pmod{n})$$

(в этом случае говорят, что 2 принадлежит показателю $n - 1$ по модулю n), то

$$m_v(x) = \sum_{r=0}^{n-1} x^{(2^n-2)r/n}.$$

Доказательство. В случае, когда $n = 1$, утверждение теоремы следует из теоремы 1, так как минимальным 2-многочленом для γ в данном случае является многочлен $x^2 - x$.

Рассмотрим случай $n > 1$. Поскольку период последовательности с общим членом d^i равен $2^n - 2$, период последовательности v делит это число, а следовательно, выполняется соотношение

$$m_v(x) \mid x^{2^n-2} - 1.$$

Пусть минимальный многочлен последовательности v имеет вид

$$m_v(x) = \sum_{t=0}^k c_t x^t.$$

Тогда, очевидно, $k \leq 2^n - 2$ и, кроме того, для любого неотрицательного i выполняется соотношение, подобное соотношению (3) из теоремы 1:

$$0 = \sum_{t=0}^k c_t v(i+t) = \sum_{t=0}^k c_t \text{tr}_2^{2^n}(\gamma \theta^{d^{i+t}}) = \sum_{t=0}^k c_t \text{tr}_2^{2^n}(\gamma (\theta^{d^i})^{d^t}).$$

Это означает, что поскольку θ^{d^i} пробегает все элементы поля $GF(2^n)$ за исключением единицы, корнями многочлена

$$C(x) = \sum_{t=0}^k c_t \text{tr}_2^{2^n}(\gamma x^{d^t})$$

будут все ненулевые элементы поля $GF(2^n)$ за исключением, быть может, единицы. Так же, как и в теореме 1, рассмотрим многочлен

$$\bar{C}(x) = C(x) \bmod (x^{2^n-1} - 1).$$

По той же схеме, как и в теореме 1, получаем, что многочлен $\bar{C}(x)$ имеет не менее $2^n - 1$ корней в поле $GF(2^n)$, однако степень его не выше $2^n - 2$. Это возможно в единственном случае, когда многочлен $\bar{C}(x)$ нулевой. Таким образом, справедливы равенства

$$\begin{aligned}\bar{C}(x) &\equiv C(x) \pmod{(x^{2^n-1} - 1)} \\ &\equiv \left(\sum_{t=0}^k c_t \text{tr}_2^{2^n}(\gamma x^{d^t}) \right) \pmod{(x^{2^n-1} - 1)} \\ &\equiv \left(\sum_{t=0}^k c_t \sum_{s=0}^{n-1} \gamma^{2^s} x^{d^t 2^s} \right) \pmod{(x^{2^n-1} - 1)} \\ &\equiv \sum_{t=0}^k c_t \sum_{s=0}^{n-1} \gamma^{2^s} x^{d^t 2^s \pmod{(2^n-1)}} = 0.\end{aligned}$$

Последнее тождество из этой цепочки перепишем в виде

$$\sum_{m=1}^{2^n-2} x^m \sum_{(t,s) \in \mathfrak{S}_m} c_t \gamma^{2^s} \equiv 0, \quad (4)$$

где во внутренней сумме суммирование ведется по всем парам из множества

$$\mathfrak{S}_m = \{(s, t) \mid 0 \leq s \leq n-1, 0 \leq t \leq k, d^t 2^s \equiv m \pmod{(2^n-1)}\}.$$

Предположим теперь, что число k (степень многочлена $m_v(x)$) строго меньше, чем $2^n - 2$. Заметим, что поскольку $2^n - 1$ — простое число, а d — примитивный элемент поля $GF(2^n - 1)$, для фиксированных s , $0 \leq s \leq n-1$, и m , $1 \leq m \leq 2^n - 2$, найдется единственное число $\tau_s^{(m)}$ такое, что

$$0 \leq \tau_s^{(m)} < 2^n - 2, \quad d^{\tau_s^{(m)}} 2^s \equiv m \pmod{(2^n-1)}.$$

Из соотношения (4) вытекает, что для любого m , $1 \leq m \leq 2^n - 2$, выполняются равенства

$$\sum_{(t,s) \in \mathfrak{S}_m} c_t \gamma^{2^s} = 0,$$

что означает, что элемент γ является корнем любого из многочленов $L_m(x)$ вида

$$L_m(x) = \sum_{s=0}^{n-1} l_{ms} x^{2^s}, \quad 1 \leq m \leq 2^n - 2,$$

где $l_{ms} = c_{\tau_s^{(m)}}$ (будем формально считать, что $c_t = 0$ при $k < t < 2^n - 2$). Выберем число m' так, чтобы выполнялись соотношения

$$0 \leq m' < 2^n - 2, \quad d^{m'} \equiv m \pmod{(2^n-2)},$$

а число δ так, чтобы выполнялись соотношения

$$0 \leq \delta < 2^n - 2, \quad d^\delta \equiv 2 \pmod{(2^n-1)}.$$

Такой выбор возможен, так как d — примитивный элемент поля $GF(2^n - 1)$. Тогда, очевидно,

$$\tau_s^{(m)} \equiv m' - s\delta \pmod{2^n - 2}$$

и многочлены $L_m(x)$ имеют вид

$$L_{m'}(x) = \sum_{s=0}^{n-1} c_{m'-s\delta} x^{2^s}, \quad 0 \leq m' < 2^n - 2, \quad (5)$$

где разность в нижнем индексе берется по модулю $2^n - 2$. Из того, что порядок элемента δ в аддитивной группе кольца Z_{2^n-2} (также как и элемента $(2^n - 2)/n$) равен n , следует, что $\delta = (2^n - 2)\beta/n$ для некоторого β .

Рассмотрим возможные случаи.

1. Начнем со случая, когда степень минимального 2-многочлена $L(x)$ элемента γ над $GF(2)$ равна 2^n . В этом случае γ не может являться корнем никакого ненулевого 2-многочлена меньшей степени. Предположим, что степень $m_v(x)$ строго меньше $2^n - 2$. Тогда γ — корень любого из многочленов (5). Значит, все они нулевые, а следовательно, все коэффициенты многочлена $m_v(x)$ равны нулю, чего быть не может. Отсюда вытекает, что в этом случае

$$m_v(x) = x^{2^n-2} - 1.$$

2. Пусть теперь степень многочлена $l(x)$, 2-ассоциированного с минимальным 2-многочленом $L(x)$ элемента γ , равна единице, что означает, что γ есть единица поля $GF(2)$. Поскольку многочлен $L(x)$ символически делит (согласно теореме 3) любой из многочленов $L_{m'}$ вида (5), каждый многочлен $L_{m'}$ либо нулевой, либо степень его не меньше 2. Ввиду очевидного равенства

$$(L_{m'}(x))^2 \equiv L_{m'}(x) \pmod{x^{2^n} - 1},$$

среди многочленов (5) всегда найдется такой, что его степень будет не меньше 2 и коэффициент при x будет отличен от нуля. Таким образом, найдутся такие числа m' и t' , что коэффициенты $c_{m'}$ и $c_{m'-t'\delta}$ будут отличны от нуля и при этом

$$m' \not\equiv m' - t'\delta \pmod{2^n - 2}.$$

Поскольку числа m' и $m' - t'\delta$ делятся на $(2^n - 2)/n$, среди коэффициентов многочлена $m_v(x)$ найдется пара ненулевых, номера которых отличаются на число, кратное $(2^n - 2)/n$. Следовательно, степень этого многочлена не меньше $(2^n - 2)/n$. Заметим, что все вышесказанное справедливо и для случаев, когда степень $l(x)$ больше единицы, но меньше n . Поэтому и в этих случаях ранг последовательности v не меньше $(2^n - 2)/n$.

Покажем теперь, что для любого натурального i выполняется соотношение

$$v(i + (2^n - 2)/n) = v(i).$$

Действительно, справедливы равенства

$$v(i + (2^n - 2)/n) = \text{tr}_2^{2^n}(\theta^{d^{i+(2^n-2)/n}}) = \text{tr}_2^{2^n}((\theta^{d^i})^{d^{(2^n-2)/n}}).$$

Как уже отмечалось, в мультипликативной группе поля $GF(2^n - 1)$ элемент $d^{(2^n-2)/n}$ имеет порядок n , причем подгруппа единственна. Поэтому существует ровно $n-1$ элемент порядка n . С другой стороны, для всех s , $1 \leq s \leq n-1$, справедливо сравнение

$$(2^s)^n \equiv 1 \pmod{2^n - 1},$$

что означает, что любой элемент порядка n , в том числе и $d^{(2^n-2)/n}$, имеет вид 2^s для некоторого s . Следовательно,

$$v(i + (2^n - 2)/n) = \text{tr}_2^{2^n}((\theta^{d^i})^{d^{(2^n-2)/n}}) = \text{tr}_2^{2^n}((\theta^{d^i})^{2^s}) = \text{tr}_2^{2^n}(\theta^{d^i}) = v(i).$$

Таким образом, последовательность v аннулируется многочленом $x^{(2^n-2)/n} - 1$, а так как ранее было показано, что степень минимального многочлена этой последовательности не меньше, чем $(2^n - 2)/n$, то

$$m_v(x) = x^{(2^n-2)/n} - 1.$$

3. Пусть теперь степень многочлена $l(x)$ меньше n , но больше единицы, и при этом 2 принадлежит показателю $n-1$ по модулю n . В этом случае $l(x)$ делит многочлен $x^n - 1$. Но последний многочлен при указанных условиях имеет только два неприводимых делителя ([1], теорема 2.47)

$$x - 1, \quad x^{n-1} + x^{n-2} + \dots + 1.$$

Следовательно, так как степень $l(x)$ больше единицы, но меньше n , выполнены равенства

$$l(x) = x^{n-1} + x^{n-2} + \dots + 1,$$

$$L(x) = x^{2^{n-1}} + x^{2^{n-2}} + \dots + x.$$

Поскольку, с одной стороны, каждый из многочленов $L_{m'}$ вида (5) делится на $L(x)$, а с другой стороны степень любого из них не выше 2^{n-1} , то либо $L_{m'}$ — нулевой многочлен, либо $L_{m'}(x) = L(x)$. Это означает, что если c_m отлично от нуля, то для любого m' , сравнимого с m по модулю $(2^n - 2)/n$, выполняется равенство $c_m = c_{m'}$. Отсюда следует, что многочлен $m_v(x)$ делится на многочлен

$$\varphi(x) = \sum_{r=0}^{n-1} x^{(2^n-2)r/n}.$$

Покажем, что этот многочлен аннулирует последовательность v . Справедливы равенства

$$\begin{aligned} \varphi(x)v(i) &= \sum_{r=0}^{n-1} x^{(2^n-2)r/n} v(i) = \sum_{r=0}^{n-1} v(i + (2^n - 2)r/n) = \sum_{r=0}^{n-1} v(i + \delta r) \\ &= \sum_{r=0}^{n-1} \text{tr}_2^{2^n}(\gamma \theta^{d^{i+\delta r}}) = \sum_{r=0}^{n-1} \text{tr}_2^{2^n}(\gamma \theta^{d^i d^{\delta r}}) = \sum_{r=0}^{n-1} \text{tr}_2^{2^n}(\gamma \theta^{d^i 2^r}) \\ &= \sum_{r=0}^{n-1} \sum_{j=0}^{n-1} \gamma^{2^j} \theta^{d^i 2^{r+j}} = \sum_{j=0}^{n-1} \gamma^{2^j} \sum_{r=0}^{n-1} \theta^{d^i 2^{r+j}} \\ &= \text{tr}_2^{2^n}(\theta^{d^i}) L(\gamma) = 0. \end{aligned}$$

Таким образом,

$$m_v(x) = \sum_{r=0}^{n-1} x^{(2^n-2)r/n},$$

что и требовалось доказать.

В случае, когда условие, состоящее в том, что 2 принадлежит показателю $n - 1$ по модулю n , не выполнено, минимальный 2-многочлен элемента γ может иметь степень меньшую, чем $2^n - 1$, и более сложное строение, что затрудняет применение рассуждений, использующих особенности структуры многочленов вида (5). Рассмотрение таких случаев является предметом дальнейших исследований.

Список литературы

1. Лидл Р., Нидеррайтер Г., *Конечные поля*. т. 1, т. 2, Мир, Москва, 1988.

Статья поступила 10.06.2002.