УДК - 004.056 + 003.26 + 519.1:004.056 Вестник УрФО № 1(23) / 2017, с. 24–27

Геут К. Л., Титов С. С.

О РЕКУРРЕНТНЫХ СООТНОШЕНИЯХ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В работе рассматриваются соотношения, задающие нелинейные рекурсии первого порядка для общего линейного рекуррентного соотношения второго порядка с постоянными коэффициентами. Авторами получены условия существования некоторых нелинейных рекурсий первого порядка для линейных рекуррентных соотношений второго порядка с постоянными коэффициентами. Проведено отслеживание количества принимаемых переменными значений, что позволяет применить полученные результаты к линейным рекуррентным соотношениям между элементами не только числовых, но и конечных полей. Рассмотрены возможные криптографические приложения в информационной безопасности.

Ключевые слова: *рекуррентное соотношение, регистр сдвига, поточный шифр, марковская цепь.*

Geut K. L., Titov S. S.

ON RECURRENT RELATIONS IN INFORMATION SECURITY

The relations that define nonlinear recursions of the first order for a general linear second-order recurrence relation with constant coefficients are considered in the article. The authors have obtained the conditions for the existence of some nonlinear recursions of the first order and linear recurrence relations of the second order with constant coefficients. Tracking the number of decisions variables the values held, this allows us to apply the results to linear recurrence relations between the elements are not only numeric, but also the finite fields. The possible cryptographic applications in information security are obtained.

Keywords: recurrence relation, shift register, stream cipher, Markov chain.

Если рассматривать рекуррентные соотношения через их разностные уравнения, решением которых является последовательность элементов поля GF(q)[1], то в результате по начальным значениям можно построить бесконечную последовательность, причем каждый ее последующий член определяется из k предыдущих. Если представить значения элементов в виде 0 и 1 из поля GF(2), то последовательности такого вида легко реализуются на компьютере.

Одна из сфер применения линейных рекуррентных соотношений – это и генерация последовательностей псевдослучайных чисел. Обычно в реальных криптосхемах линейный регистр сдвига с обратной связью реализуется одной из двух различных конструкций, называемых, соответственно, регистрами Фибоначчи и Галуа, но все наиболее важные теоретические результаты применимы к обоим типам.

Еще один пример – рекуррентное распределение вероятностей марковских цепей[2], которые используются как математический аппарат для описания, например, процесса несанкционированной атаки, распознавания речи, аутентификации.

Использование рекуррентных соотношений над конечными полями для М-последовательностей при генерации гаммы шифров дает максимальный период, что влияет на стойкость шифра. Криптостойкость поточных шифров полностью зависит от качества генератора потока ключей. Большинство современных генераторов гаммы построено на линейных регистрах сдвига (ЛРС). Главная проблема при проектировании структуры ЛРС – это достижение максимального периода повтора ЛРС, потому что повтор состояния ЛРС означает, что и гамма будет периодически повторяться, что снижает криптостойкость системы. Для ЛРС длиной n бит максимальный период составляет $2^n - 1$ тактов (состояние, когда все биты равны нулю, недопустимо, поскольку ЛРС любой структуры не выходит из этого состояния, зацикливаясь в нем).

Существуют генераторы, порождающие нелинейные рекуррентные последовательности, такие генераторы по своим диагностическим свойствам отличаются от линейных. В частности, в n-разрядном нелинейном генераторе достаточно просто порождается двоичная последовательность де Брейна. Она представляет собой нелинейную двоичную последовательность x_i периода $T = 2^n$, в которой всевозможные векторы $(x_j, x_{j+1}, \ldots x_{j+n-1})$ длины n при любом j встречается только один раз. Исключение запрещенного нулевого состояния всех триггеров генератора позволяет увеличить период формируемой последовательности и сделать его максимально возможным, равным 2^m, повысить ее качество, так как вероятности появления 0 и 1 становятся равными 0,5. На основе таких последовательностей построен, в частности, циклический избыточный код CRC32.

Одна из классических задач рекуррентных последовательностей – числа Фибоначчи, которые удовлетворяют линейному рекуррентному соотношению второго порядка. В работе В. Н. Ушакова[3] была поставлена и решена задача построения нелинейной рекурсии первого порядка для таких чисел: $u_{n+2} = u_{n+1} + u_n$.

$$u_{n+1} = \frac{1}{2}u_n + \frac{1}{2}\sqrt{5u_n^2 - 4}\ , \text{при нечетном n,} \quad (1)$$

$$u_{n+1} = \frac{1}{2}u_n + \frac{1}{2}\sqrt{5u_n^2 + 4}\ , \text{при четном n.} \quad (2)$$

Общая задача понижения порядка рекуррентного соотношения ставится для произвольной рекурсии.

Рассмотрим линейное уравнение конечных разностей 2-го порядка с постоянными коэффициентами и без правой части[1].

$$f_{x+2} + a_1 f_{x+1} + a_2 f_x = 0. \quad (3)$$

Один из примеров решения такого уравнения – числа Фибоначчи:

$$u_{n+2} = u_{n+1} + u_n, \quad (4)$$

где $u_1 = u_2 = 1$[1].

Решаем это рекуррентное соотношение стандартным образом[1] и получаем итоговую формулу:

$$x = u_n = \ë^n = \frac{f_n \pm \sqrt{f_n^2 - 4a_2^n C_1 C_2}}{2C_1}. \quad (5)$$

Если $a_2 = 1$, то x есть функция одной переменной f_n при постоянных C_1 и C_2.

Если $a_2 = -1$, то x есть функция одной переменной f_n, но разного вида для четных и нечетных n.

Если $a_2^3 = 1$, т.е. порядок a_2 равен трем, то x есть функция одной переменной f_n, но трех видов, в зависимости от остатка деления n на три.

Если $a_2^4 = 1$ (например, $a_2 = i$), т.е. порядок a_2 равен четырем, то x есть функция одной переменной f_n, но четырех видов и т.д.

Если же порядок a_2 бесконечный, то нет единой формулы, и x есть функция двух переменных f_n и n.

Предположим, что порядок a_2 конечный. Решение задачи построения рекурсии первого порядка аналогично задаче нахождения промежуточных интегралов первого порядка для дифференциальных уравнений второго порядка. В этом случае получаем

$$f_{n+1} = C_1 \ë^{n+1} + C_2 \frac{a_2^{n+1}}{\ë^{n+1}} \quad (6)$$

Это и есть решение в общем виде.

$$f_{n+1} = C_1 \frac{f_n + \sqrt{f_n^2 - 4a_2^n C_1 C_2}}{2C_1} \ë + C_2 \frac{2C_1 a_2^{n+1}}{\ë(f_n + \sqrt{f_n^2 - 4a_2^n C_1 C_2})} \quad (7)$$

Утверждение 1. Если в квадратном уравнении $\lambda^2 + a_1\lambda^1 + a_2 = 0$ порядок свободного члена конечен и равен *p*, то для решения рекуррентного соотношения при заданных C_1, C_2 корень $x = \lambda^n$ является функ- $f_{n+1} = C_1\ë_1^{n+1} + C_2\ë_2^{n+1}$ цией одной переменной fn и задается формулой p видов.

Более общая задача, когда $\lambda = 0$ или $\lambda = 1$ тоже сводится к зависимости первого порядка. В общем случае требуется описать, какие должны быть коэффициенты характеристического уравнения, чтобы существовала зависимость в виде многочлена.

Так, квадратичная зависимость, вида

$F(f_n, f_{n+1}) = af_n^2 + bf_nf_{n+1} + cf_{n+1}^2 + df_n + ef_{n+1} = C = Const$ (8)

имеет место при

$fn = C1\lambda_1^n + C2\lambda_2^n$,

$= u \quad = v$

$fn+1 = C1\lambda_1^{n+1} + C2\lambda_2^{n+1}$.

$= \lambda 1u \quad = \lambda 2v$

Эта зависимость (8) при $\lambda_1 = -1, \lambda_2 \notin \{0,1,-1\}$ существует в виде $\lambda_2^2 f_n^2 - 2\lambda_2 f_n f_{n+1} + f_{n+1}^2 = C$ (9)

для рекуррентного соотношения

$$f_{n+2} - (\lambda_2 - 1)f_{n+1} - \lambda_2 f_n = 0 \quad (10)$$

Кубическая зависимость первого порядка вида

$F(f_n, f_{n+1}) = af_n^2 + bf_nf_{n+1} + cf_{n+1}^2 + df_n + ef_{n+1} = C = Const$ (11)

должна выполняться тождественно по n для функций

$fn = C_1\lambda_1^n + C_2\lambda_2^n = u + v$,

$fn+1 = C_1\lambda_1^{n+1} + C_2\lambda_2^{n+1} = \lambda_1 u + \lambda_2 v$,

$(\lambda_1 \neq \lambda_2)(\lambda_i \notin \{0,1,-1\}) \quad (\lambda_1\lambda_2 \neq 1)$

Решение на основании определителей типа Вандермонда показывает, что такая зависимость может иметь место, только если либо $\lambda_1 = \lambda_2$, либо $\lambda_1 = 1$, либо $\lambda_2 = 1$, чего не может быть по предположению.

Итак, доказано

Утверждение 2. Кубическая зависимость (11) имеет место (при отсутствии квадратичной), только в случае, когда корни λ_1, λ_2 характеристического уравнения удовлетворяют либо уравнению $\lambda_1^2\lambda_2 = 1$, либо уравнению $\lambda_1\lambda_2^2 = 1$. При этом зависимость оказывается однородной.

Использование рекуррентных соотношений дает эффективный метод решения многих комбинаторных задач. В криптографии рекуррентные соотношения используются для генераторов псевдослучайных последовательностей.

Проведённое выше отслеживание количества принимаемых переменными значений позволяет применить полученные результаты и к линейным рекуррентным соотношениям между элементами не только числовых, но и конечных полей. Так, обобщение соотношения Чебышёва для многочленов Чебышёва-Диксона[5,6] может прояснить проблему с простыми числами Ферма[7] для которых задача дискретного логарифмирования предполагается быстро решаемой.

Примечания

1. Гельфонд А. О. Исчисление конечных разностей / М.: Наука, 1967. – 376 с.

2. Марков А. А. Исчисление конечных разностей / Одесса : Типография Акционерного Южно-Русского Общества Печатного Дела, 1910.

3. Ушаков В. Н. Египетские треугольники и числа Фибоначчи // Империя математики. – №1. – 2001. – С. 21–60.

4. Геут Кр. Л., Титов С. С. Задача, эквивалентная проверке простоты чисел Ферма // Прикладная дискретная математика (Приложение). – Томск: ТПУ. 2014. – № 7. – С. 13–14.

5. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М. : КомКнига, 2012. – 328 с.

6. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М. : КомКнига. 2006. – 280 с.

7. Геут К. Л., Титов С. С. О задаче построения нелинейных рекуррентных соотношений // IV междисциплинарная молодежная научная конференция УрО РАН «Информационная школа молодого ученого» : сб. научных трудов ЦНБ УрО РАН. – Екатеринбург, 2014. – С. 203–208.

8. Бабаш А. В., Шанкин Г. П. Криптография. под редакцией В. П. Шерстюка, ЭЛ. Применко – М. : СОЛОН-ПРЕСС. 2007 – 512 С.

ГЕУТ Кристина Леонидовна, ассистент Уральского государственного университета путей сообщения, 620034, Екатеринбург, ул. Колмогорова, д. 66, E-mail: geutkrl@yandex.ru

ТИТОВ Сергей Сергеевич, профессор Уральского государственного университета путей сообщения, докт. физ-мат. наук, профессор, 620034, Екатеринбург, ул. Колмогорова, д. 66, E-mail: sergey.titov@usaaa.ru

GEUT Kristina Leonidovna, Assistant professor of the Ural State University of Railway Transport, 620034, 66 Bld., Kolmogorova Str., Ekaterinburg, E-mail: geutkrl@yandex.ru

TITOV Sergey Sergeevich, Professor of the Ural State University of Railway Transport, Doctor of Physical and Mathematical Sciences, Professor, 620034, 66 Bld., Kolmogorova Str., Ekaterinburg, E-mail: sergey.titov@usaaa.ru