ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ЗАЩИТА ИНФОРМАЦИИ

УДК 519.6

И. П. Кобяк, канд. техн. наук
Белорусский государственный университет
информатики и радиоэлектроники
(Республика Беларусь, 220600, Минск, ул. П. Бровки 6,
тел. 293-86-17; E-mail1: MatvienkoI.I@list.ru, E-mail2: IPKobyak@mail.ru)

Аналитический синтез членов псевдослучайной последовательности на основании многочленов разбиений

(Статью представил д-р техн. наук В. В. Мохор)

Выполнен анализ методов генерирования псевдослучайных чисел с использованием полиномов над полем $GF(2m)$. На основании свойств полиномиальных коэффициентов получено и доказано равенство для общего члена M-последовательности, указана область применения тождеств, соответствующих полученной канонической модели. Показано, что частные реализации многочленов Белла, порождаемые ограниченным набором коэффициентов полинома, также удовлетворяют линейным рекуррентным соотношениям.

Виконано аналіз методів генерування псевдовипадкових чисел з використанням поліномів над полем $GF(2m)$. На базі властивостей поліноміальних коефіцієнтів отримано та доведено рівність для загального члена M-послідовності, вказано область застосування тотожностей, відповідних до отриманої канонічної моделі. Показано, що окремі реалізації многочленів Белла, породжувані обмеженим набором коефіцієнтів полінома, також задовольняють лінійним рекурентним співвідношенням.

К л ю ч е в ы е с л о в а: моделирование генераторов чисел, многочлены разбиений, рекурсивность, задачи диагностики, факториальные тождества, абстрактные объекты.

Постановка задачи. Моделирование рекуррентных объектов может быть успешно использовано в задачах экономики, кибернетики (машина синтезирует машину), искусственного интеллекта (алгоритм модифицирует алгоритм). В работе [1] сформулирована следующая теорема о рекурсивности: если жизнеспособная система содержит в себе жизнеспособную систему, то их воспроизводящие структуры являются рекурсивными. Это утверждение представляет собой одно из биотехнических обобщений идей генерирования абстрактных и реальных объектов, которое может быть использовано при построении интеллектуальных систем с принципиально новым кибернетическим началом. Применяя идею рекурсивности и соответствующий математический подход для решения практических задач [2, 3], предполагают,

что некоторая вычислительная среда, реализуя механизмы сканирования и преобразования входных данных, может осуществлять расчеты коэффициентов линейной рекуррентной последовательности, фрагмент которой будет соответствовать зарегистрированному описанию действительности. При этом априорно учитывается гипотеза о возможном нарушении псевдослучайности в случае интерпретации сообщений полиномами малых степеней m, однако считается, что наблюдаемый набор двоичных событий, в конечном итоге, может быть отождествлен с фрагментом M-последовательности после k-кратного увеличения степени многочлена (до значения $m_k > m$), использованного предварительно для моделирования наблюдаемой реальности. В качестве вспомогательного механизма адаптации интеллектуальной среды к псевдорекуррентности входной информации может быть использована методология накопления знаний. Согласно данной концепции предполагается, что некоторый центральный генератор («разнообразия» [1]) в процессе фонового функционирования будет формировать в качестве наполнителей слотов запоминающих устройств участки рекуррентных последовательностей с определенными свойствами, удовлетворяющие генераторным полиномам различных степеней. Если при этом вновь наблюдаемый информационный объект не будет принадлежать ни одной из реализаций накопленной базы, то, по возможности, должно быть выполнено увеличение степени порождающего многочлена (или центрального источника), что эквивалентно усложнению моделируемой в интеллектуальной среде информационной обстановки.

Однако моделирование аппаратуры или программирование известных методов, связанных с рекурсивной генерацией требует весьма существенных временных затрат. Формирование и анализ последовательностей, принадлежащих полиномам степени $m = 80 \div 100$, в большинстве практических приложений оказывается невозможным, так как длительность решения подобных задач на компьютере может измеряться годами. Другая проблема, стоящая перед разработчиками систем, основанных на использовании рекурсивного, а в общем случае полиномиально-комбинаторного принципа [3], заключается в проверке безошибочности формируемых объектов при использовании в качестве источника выборки генераторов большой разрядности. В этом случае оказывается целесообразным дублирование методов синтеза псевдослучайных событий, так как моделирование двоичных устройств на универсальных компьютерах — достаточно трудоемкая задача.

Таким образом, проблема синтеза элементов генеральной совокупности псевдослучайных объектов по их номеру или в соответствии с формулой общего члена достаточно актуальна и является одним из необходимых условий решения ряда задач прикладного и теоретического характера.

Методы синтеза общего члена псевдослучайной последовательности и их недостатки. Существующие методы определения членов линейной рекуррентной последовательности R_n по заданному номеру $n = 0, 1, 2, 3 \ldots$ имеют существенные недостатки как субъективного, так и объективного характера.

Во-первых, в известных классических соотношениях [4] отсутствует явно выраженная зависимость значений R_n от коэффициентов порождающего полинома $\varphi(x)$, определенного над полем $GF(2^m)$:

$$\varphi(x) = 1 \oplus \alpha_1 x^1 \oplus \alpha_2 x^2 \oplus \ldots \oplus \alpha_m x^m, \alpha_i \in \{0,1\}. \quad (1)$$

Данный факт исключает функциональную очевидность результатов и используемого алгоритма для синтеза n-го члена M-последовательности, что при экспериментальном или практическом использовании генераторов усложняет восприятие и развитие теоретических наработок.

Во-вторых, общий член R_n может быть выражен через корни многочлена (1). При этом используются классические результаты и соотношения теории полей, теории колец или групп [4]. На практике синтезом рекуррентных последовательностей приходится заниматься не математикам-теоретикам, а инженерам-разработчикам аппаратуры, решающим задачи диагностики, надежного хранения информации или идентификации последовательностей. При этом ограничения в номенклатуре моделей генераторов псевдослучайных последовательностей (ПСП) существенно снижают уровень разработок и новых проектов систем. Таким образом, требуется синтез методов дискретных преобразований, программирование которых не вызывало бы затруднений.

Третий недостаток обусловлен известной методологией вычисления значений R_n как произведения строго определенного начального вектора $\mathbf{R}_0 = (R_0, R_j = 0), j = 1, 2, \ldots, m-1$, и ряда сопровождающих матриц [5, 6], возведенных в заданную степень. Очевидно, что данный алгоритм при больших значениях m, а следовательно, и сверхбольших длинах периода $M \le r^m - 1$, где r — основание системы счисления (так как рекуррентность свойственна не только 0,1-объектам), оказывается неприменим из-за существенной сложности формирования произведения матриц размера $m \times m$ и их размещения в памяти. Применение современных высокоскоростных процессоров для решения данной задачи не снижает сложности программирования, а является лишь средством повышения производительности вычислений. Следует также заметить, что методология формирования членов рекуррентной последовательности с использованием матричных алгоритмов не позволяет записать общую формулу для R_n. Это связано с тем, что произведение ряда матриц в общем случае трудно формализуется и не приводит к простым аналитическим зависимостям.

Таким образом, с учетом изложенных ограничений и недостатков решим задачу синтеза общего члена линейной рекуррентной последовательности как функции коэффициентов порождающего полинома $R_n = f(\alpha_i)$, используя теоретико-числовой аспект и понятие многочленов разбиений [7].

Вывод факториальной формы общего члена линейной рекуррентной последовательности. Положим $R_0 = 1$ и выполним простую подстановку взамен данного значения коэффициента α_1 полинома (1), взятого в нулевой степени, т. е. определим начальное равенство

$$R_0 = \alpha_1^0. \tag{2}$$

Вычислим значение $\mathbf{R}_1$, применяя к вектору $\mathbf{R}_0$ принцип псевдослучайного генерирования в соответствии с формулой

$$R_1 = \sum_{i=1}^{m} \alpha_i R_{1-i}, \; R_{1-i} = 0, \; i = \overline{2,m}. \tag{3}$$

Здесь и далее все действия выполняются над полем целых чисел. Подставляя (2) в соотношение (3), легко получить равенство

$$R_1 = \alpha_1^1 + \sum_{i=2}^{m} \alpha_i \cdot 0 = \alpha_1^1 . \tag{4}$$

Очередной член линейной рекуррентной последовательности может быть также получен на основании равенства (3), но с использованием уже известных значений (2) и (4):

$$R_2 = \sum_{i=1}^{m} \alpha_i R_{2-i} = \alpha_1^2 + \alpha_1^0 \alpha_2^1 .$$

Для члена R_3 получаем равенство

$$R_3 = \sum_{i=1}^{m} \alpha_i R_{3-i} = \alpha_1^3 + 2\alpha_1^1 \alpha_2^1 + \alpha_1^0 \alpha_3^1 .$$

Аналогичная методика после n-кратного применения приводит к многочлену вида

$$R_n = \sum_{\pi(n)} \frac{k(n)!}{k_{1,n}!k_{2,n}!...k_{m,n}!} \alpha_1^{k_{1,n}} \alpha_2^{k_{2,n}} ... \alpha_m^{k_{m,n}} , \tag{5}$$

где суммирование выполняется по всем разбиениям $\pi(n)$ числа n на составляющие $k_{1,n}, k_{2,n}, ..., k_{m,n}$; $n = 1k_{1,n} + 2k_{2,n} + ... + mk_{m,n}$; $k(n) = k_{1,n} + k_{2,n} + ... + k_{m,n}$.

Докажем приведенное соотношение по индукции. Очевидно, что для $(n-i)$-го члена последовательности, определяемой согласно (5), справедливо равенство

$$R_{n-i} = \sum_{\pi\,(n-i)} \frac{k\,(n-i)!}{k_{1,\,n-i}!k_{2,\,n-i}!...k_{m,\,n-i}!}\,\alpha_1^{k_{1,n-i}}\alpha_2^{k_{2,n-i}}...\alpha_m^{k_{m,n-i}}.$$

Используя рекуррентный принцип формирования псевдослучайных чисел, можно записать

$$R_n = \sum_{i=1}^{m}\alpha_i \sum_{\pi\,(n-i)} \frac{k\,(n-i)!}{k_{1,\,n-i}!k_{2,\,n-i}!...k_{m,\,n-i}!}\,\alpha_1^{k_{1,n-i}}\alpha_2^{k_{2,n-i}}...\alpha_m^{k_{m,n-i}}. \qquad (6)$$

При этом умножение α_i на соответствующие многочлены разбиений R_{n-i} приводит к факториальному соотношению

$$R_n = \sum_{\pi\,[(n+1)-1]} \frac{k(n-1+1)!}{(k_{1,\,n-1}+1)!k_{2,\,n-1}!...k_{m,\,n-1}!}\,\alpha_1^{k_{1,n-1}+1}\alpha_2^{k_{2,n-1}}...\alpha_m^{k_{m,n-1}} +$$

$$+ \sum_{\pi\,[(n+1)-2]} \frac{k\,(n-2+1)!}{k_{1,\,n-2}!(k_{2,\,n-2}+1)!...k_{m,\,n-2}!}\,\alpha_1^{k_{1,n-2}}\alpha_2^{k_{2,n-2}+1}...\alpha_m^{k_{m,n-2}} + ...$$

$$... + \sum_{\pi\,[(n+1)-m]} \frac{k\,(n-m+1)!}{k_{1,\,n-m}!k_{2,\,n-m}!...(k_{m,\,n-m}+1)!}\,\alpha_1^{k_{1,n-m}}\alpha_2^{k_{2,n-m}}...\alpha_m^{k_{m,n-m}+1}. \qquad (7)$$

Используя определение (5), можно показать, что между степенями коэффициентов α_i и индексами $(n-i)$ в (7) существуют следующие математические и статистические связи. Умножение многочлена R_{n-1} на коэффициент α_1 полинома $\varphi\,(x)$ приводит к образованию суммы

$$1(k_{1,\,n-1}+1)+2k_{2,\,n-1}+...+mk_{m,\,n-1}=n, \qquad (8)$$

где $(k_{1,\,n-1}+1)+k_{2,\,n-1}+...+k_{m,\,n-1}=k_{1,\,n}+k_{2,\,n}+...+k_{m,\,n}=k\,(n)$, т. е. слагаемое $1(k_{1,\,n-1}+1)$ в (8) все разбиения $\pi\,(n-1)$ числа $n-1$ автоматически трансформирует в разбиения $\pi\,(n)$,

$$(k_{1,\,n-1}+1), k_{2,\,n-1}, ..., k_{m,\,n-1} \to k_{1,\,n}, k_{2,\,n}, ..., k_{m,\,n} \in \pi\,(n). \qquad (9)$$

Аналогично при $i=2$ разбиения $\pi\,(n-2)$ становятся разбиениями $\pi\,(n-1)$:

$$k_{1,\,n-2}, (k_{2,\,n-2}+1), ..., k_{m,\,n-2} \to k_{1,\,n-1}, k_{2,\,n-1}, ..., k_{m,\,n-1} \in \pi\,(n-1). \qquad (10)$$

Однако, учитывая соотношение $1k_{1,\,n-2}+2\,(k_{2,\,n-2}+1)+...+m\,k_{m,\,n-2}=n$, можно констатировать, что $k_{1,\,n-2}+(k_{2,\,n-2}+1)+...+k_{m,\,n-2}=k\,(n-1)$ принадлежат сум-

ме $k(n)$ с разбиениями $k_{1,n-1}, k_{2,n-1}, ..., k_{m,n-1} \to k_{1,n}, k_{2,n}, ..., k_{m,n} \in \pi(n)$, но для определенного подмножества значений $k(n)$. В граничном варианте при $i = m$ соотношения

$$\begin{gathered} k_{1,n-m} + 2k_{2,n-m} + ... + m(k_{m,n-m} + 1) = n, \\ k_{1,n-m} + k_{2,n-m} + ... + (k_{m,n-m} + 1) = k(n-m+1) \in \pi(n), \end{gathered} \tag{11}$$

т. е. $k_{1,n-m}, k_{2,n-m}, ..., (k_{m,n-m}+1)$, трансформируются в подмножество разбиений $\pi(n-m+1)$ числа $n-m+1$, равное $k_{1,n-m+1}, k_{2,n-m+1}, ..., k_{m,n-m+1}$ которые, в свою очередь, входят в состав множества разбиений $\pi(n)$ числа n как некоторое подмножество $k_{1,n}, k_{2,n}, ..., k_{m,n}$.

В соотношениях (8)—(11) используются одинаковые обозначения для чисел $k(n)$, однако сами значения $k(n)$ и соответствующие им разбиения различны. Тождественность обозначений следует из формального представления генератора в виде соотношения (5), где множества аргументов $k_{1,n}, k_{2,n}, ..., k_{m,n}$ отождествляются в составляющих суммы свои аргументы $k(n)$ для каждого из разбиений.

Таким образом, все представления чисел $k(n-i)$ в виде разбиений $\pi(n-i)$ при умножении многочлена R_{n-i} на соответствующий коэффициент α_i автоматически оказываются составными частями чисел $k(n)$ с разбиениями $\pi(n)$, а также составляющими чисел $k(n-i+1) \in \pi(n-i+1)$. Например, элемент l-го члена последовательности $N\alpha_p^q \alpha_n^t$, $l = qp + tn$, при умножении на коэффициент α_r^s будет представлять собой элемент многочлена степени $l + sr$.

Итак, на основании тождества (6) получаем общую запись (7) в виде

$$R_n = \sum_{\pi[(n+1)-i]} \frac{k(n+1-i)!}{k_{1,n+1-i}!k_{2,n+1-i}!...k_{m,n+1-i}!} \alpha_1^{k_{1,n+1-i}} \alpha_2^{k_{2,n+1-i}} ... \alpha_m^{k_{m,n+1-i}} =$$

$$= \sum_{\pi(n)} \frac{k(n)!}{k_{1,n}!k_{2,n}!...k_{m,n}!} \alpha_1^{k_{1,n}} \alpha_2^{k_{2,n}} ... \alpha_m^{k_{m,n}} . \tag{12}$$

Равенства (5) и (12) эквивалентны. Следовательно, факториальное соотношение (5) можно считать доказанным по индукции.

Доказательство рекурсивности частных полиномов Белла на ограниченном наборе аргументов. Приведенное выше доказательство позволяет также выявить рекурсивность полиномов Белла $B_{n,k}$ на ограниченном наборе аргументов $k_{i,n}$ (при $i = \overline{1,m}$), представляющих собой известный инструмент исследования числовых рядов.

В равенстве (6) значения $k(n-i)$ представляют собой функциональную зависимость вида $f(n-i)$. Поэтому выполним замену аргументов

данной функции аргументами, суммирование которых в (6) будет осуществляться в соответствии с равенством $k(n-j)=k_{1,n}+k_{2,n}+...+k_{m,n}$, где $k(n-j)=\text{const}$, в разбиениях чисел $n-i$.

Процесс преобразования соотношения (6) рассмотрим на следующем примере. Пусть разрядность формирователя рекуррентной последовательности $m = 3$ и $\varphi(x)=1+\alpha_1 x^1+\alpha_2 x^2+\alpha_3 x^3$. Тогда все составляющие для члена R_n, равного, например, R_5, могут быть образованы умножением множеств разбиений чисел 4, 3 и 2 для членов R_{5-1}, R_{5-2} и R_{5-3} соответственно на коэффициенты α_1, α_2, α_3. Если произведения в столбцах табл. 1 упорядочить в соответствии с суммой степеней коэффициентов α_i для данного n, то процесс замены суммы элементов строк, образуемых по формуле (5) при $m=3$, суммой элементов столбцов оказывается очевиден, что подтверждается результатами [7]. С учетом указанных преобразований из тождеств (5) и (12) следует соотношение

$$R_n=\sum_{\pi(n)}\sum_{j=0}^{m}\frac{k(n-j)!}{k_{1,n}!k_{2,n}!...k_{m,n}!}\alpha_1^{k_{1,n}}\alpha_2^{k_{2,n}}...\alpha_m^{k_{m,n}},$$
$$k(n-j)=k_{1,n}+k_{2,n}+...+k_{m,n}=\text{const},\ \ n=1k_{1,n}+2k_{2,n}+...+mk_{m,n}, \tag{13}$$

где $k(n-j)$ — константные значения для некоторого подмножества разбиений числа n; аналогичный параметр $k(n-i)$ в формуле (6) представляет собой сумму разбиений числа $n-i$.

Известно, что сумма факториальных составляющих в (13)

$$B_{n,k(n-j)}=\sum_{\pi(n)}\frac{k(n-j)!}{k_{1,n}!k_{2,n}!...k_{n,n}!}\alpha_1^{k_{1,n}}\alpha_2^{k_{2,n}}...\alpha_m^{k_{n,n}} \tag{14}$$

представляет собой полиномы Белла при $k(n-j)=\text{const}$. Следовательно, подставляя тождество (14) в общий член (13), при всех значениях $\alpha_j=0$, $j=\overline{m+1,n}$, получаем соотношение

$$R_n=\sum_{j=0}^{m}B_{n,k(n-j)}. \tag{15}$$

Таблица 1

$n-3=2$	$\times\alpha_3\to 0$	$0\quad 0$	α_1^2	α_2^1
$n-2=3$	$\times\alpha_2\to 0$	$\alpha_1^3\quad 0$	$2\alpha_1^1\alpha_2^1$	α_3^1
$n-1=4$	$\times\alpha_1\to\alpha_1^4$	$3\alpha_1^2\alpha_2^1$	$2\alpha_1^1\alpha_2^1\quad\alpha_2^2$	
$n=5$	$\alpha_1^5\quad 4\alpha_1^3\alpha_2^1$	$3\alpha_1^2\alpha_3^1\quad 3\alpha_1^1\alpha_2^2$	$2\alpha_2^1\alpha_3^1$	

Поскольку тождество (15) образовано из (13), можно утверждать, что перегруппировка $B_{n,k(n-j)}$ приводит к соотношению (5), которое является рекурсивным. Следовательно, на основании тождества (6) можно записать

$$R_n = \sum_{i=1}^{m} \alpha_i \sum_{j=0}^{m} B_{n-i,k(n-i-j)}. \tag{16}$$

Очевидно, что в равенстве (16) общий член R_n равен сумме:

$$R_n = \alpha_1 \sum_{j=0}^{m} B_{n-1,k(n-1-j)} + \alpha_2 \sum_{j=0}^{m} B_{n-2,k(n-2-j)} + \ldots + \alpha_m \sum_{j=0}^{m} B_{n-m,k(n-m-j)} =$$

$$= \sum_{j=0}^{m} \left[\frac{k(n-j)!}{(k_{1,n-1}+1)!k_{2,n-1}!\ldots k_{m,n-1}!} \alpha_1^{k_{1,n-1}+1} \alpha_2^{k_{2,n-1}} \ldots \alpha_n^{k_{m,n-1}} + \right.$$

$$+ \frac{k(n-j)!}{k_{1,n-2}!(k_{2,n-2}+1)!\ldots k_{m,n-2}!} \alpha_1^{k_{1,n-2}} \alpha_2^{k_{2,n-2}+1} \ldots \alpha_n^{k_{m,n-2}} + \ldots$$

$$\left. + \frac{k(n-j)!}{k_{1,n-m}!k_{2,n-m}!\ldots(k_{m,n-m}+1)!} \alpha_1^{k_{1,n-m}} \alpha_2^{k_{2,n-m}} \ldots \alpha_n^{k_{m,n-m}+1} \right].$$

Данное тождество является общим для всех строк и столбцов табл. 1, составленной для произвольного значения n. Тогда, с учетом (8) — (11), можно записать соотношение

$$R_n = \sum_{j=0}^{m} \frac{k(n-j)!}{k_{1,n}!k_{2,n}!\ldots k_{m,n}!} \alpha_1^{k_{1,n}} \alpha_2^{k_{2,n}} \ldots \alpha_n^{k_{m,n}} = \sum_{j=0}^{m} B_{n,k(n-j)}.$$

Подставляя в факториальное тождество (14) значение $j = 0$, получаем соответствие равенства (5) и полиномов Белла $B_{n,k(n)}$:

$$B_{n,k(n)} = \sum_{i=1}^{m} \alpha_i B_{n-i,k(n-i)},$$

т. е. многочлены $B_{n,k(n)}$ (14) оказываются рекурсивными, так же как и члены ПСП R_n.

Пример. Пусть $m = 5$, $\phi(x) = 1 \oplus x^1 \oplus x^2 \oplus x^4 \oplus x^5$. Требуется определить $R_{n=11}$, используя факториальное тождество (5). Учитывая, что в качестве начального состояния генератора берется строго определенный вектор $\mathbf{R}_0 = 100..00$, а $a_i \in \{0,1\}$, получаем значение бита с номером 11, используя принцип аппаратного формирования членов M-последовательности. Очевидно, что в данном случае $R_{n=11} = 0$.

Таблица 2

$\pi(11)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$k_{1,11}$	1	0	2	0	2	4	6	1	3	1	3	5	7	1	3	5	7	9	11
$k_{2,11}$	0	1	0	3	2	1	0	1	0	3	2	1	0	5	4	3	2	1	0
$k_{4,11}$	0	1	1	0	0	0	0	2	2	1	1	1	1	0	0	0	0	0	0
$k_{5,11}$	2	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
$R_{11} \bmod 2$	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1

На основании соотношения (5) запишем тождество

$$R_{11} = \sum_{\pi(n)} \frac{k(n)!}{k_{1,n}!k_{2,n}!\ldots k_{m,n}!} = \sum_{\pi(11)=19} \frac{k(n)!}{k_{1,11}!k_{2,11}!k_{4,11}!k_{5,11}!}.$$

Все разбиения для данного значения n определены из уравнения $1k_{1,11} + 2k_{2,11} + 4k_{4,11} + 5k_{5,11} = 11$ и представлены в табл. 2.

Используя данные табл. 2, записываем факториальные моменты, определяющие нечетные составляющие члена $R_{n=11} = \sum_{\pi(11)} R_{11} \bmod 2$ и вносящие над полем GF(2) единичный вклад в сумму

$$R_{n=11} = \frac{3!}{1!2!} + \frac{7!}{6!1!} + \frac{7!}{3!4!} + \frac{11!}{11!} = 3 + 7 + 35 + 1 = 46 = 0 \bmod 2.$$

Значения битов, полученные с помощью генератора псевдослучайных чисел n тактов и рассчитанные по формуле (5), точно совпадают. Таким образом, соотношение для общего члена доказано на практическом примере.

Выводы. Полученное соотношение для общего члена рекуррентной ПСП имеет явно выраженную зависимость от коэффициентов порождающего полинома. Это дает возможность при программной реализации генераторов формировать числа R_n по достаточно простому алгоритму. Наличие в доказанном соотношении только комбинаторных тождеств исключает необходимость специальной подготовки программистов, так как природа формируемых рекуррентных объектов очевидна.

Применение полученного результата будет эффективным при решении задач формирования и идентификации случайной выборки, где требуется синтезировать отсчеты генеральной совокупности псевдослучайных объектов, принадлежащих достаточно большим номерам n. Следует заметить, что результаты моделирования на компьютере двух различных методов формирования чисел — базового (1) и оригинального — показали, что трехчлены вида (1) и (5) конкурируют в области временных параметров, невзирая на близкую к *NP*-полной природу предлагаемой вычислительной процедуры (5).

В прикладных задачах моделирования искусственного интеллекта [2, 3] наиболее важным моментом является проблема сжатия и формирования подпоследовательностей. Однако в данном случае формируемые объекты должны иметь некоторые априорно заданные статистические свойства, в связи с чем возникает задача подбора членов. Формула (5) может быть использована для программной проверки (0, 1)-событий при решении подзадач синтеза интегральных кодов, «развертывание» которых создает эффект лавинообразного запуска (аналогично «нейронному» запоминающему устройству) механизмов восстановления информации [3].

Полученный результат позволяет рассматривать предложенную методологию синтеза рекуррентных объектов как базовую и открывает возможность применения к M-последовательностям любых известных комбинаторных методов анализа.

The analysis of the methods of pseudorandom numbers generation having used of polynomials over the $GF(2^m)$ field is performed. The equality for general member of M-sequence is obtained and proved on the basis of polynomial coefficient properties. The application domain identities which correspond the obtained canonical model is indicated. It is demonstrates that particular realizations of Bell polynomials which was generated by the limited set of polynomial coefficients satisfy to linear recurrent relationship.

1. *Бир С.* Мозг фирмы/ Пер.с англ. — М. : Радио и связь, 1993.
2. *Амосов Н. М., Касаткин А. М., Касаткина Л. М., Талаев С. А.* Автоматы и разумное поведение. — Киев : Наук. думка, 1973.
3. *Кобяк И. П.* Системные средства для сжатия\восстановления данных в подсистемах запоминающих устройств интеллектуальных вычислительных систем// АВТ.— 2001. — № 2. — С. 51—61.
4. *Лидл Р., Ниддеррайтер Г.* Конечные поля. В 2-х томах/ Пер. с англ. — М. : Мир, 1988.
5. *Ланкастер П.* Теория матриц / Пер. с англ. — М. : Наука, 1982.
6. *Яковлев В. В., Федоров Р. Ф.* Стохастические вычислительные машины. — Л. : Машиностроение, 1974.
7. *Риордан Дж.* Комбинаторные тождества. — М : Наука, 1982.

Поступила 10.12.07

КОБЯК Игорь Петрович, канд. техн. наук, доцент кафедры ЭВМ Белорусского государственного университета информатики и радиоэлектроники (г. Минск). В 1982 г. окончил Минский радиотехнический ин-т (ныне БГУИР). Область научных исследований – прикладные вопросы математической статистики, методы испытания цифровой техники, проектирование высокопроизводительных компьютерных систем.