О ДВУХ КЛАССАХ АВТОМАТОВ НАД КОНЕЧНЫМИ КОЛЬЦАМИ, ПОСТРОЕННЫХ НА ОСНОВЕ ИЗОМОРФИЗМА РЕГИСТРА СДВИГА С ПЕРЕНОСОМ, И ИХ ПРИМЕНЕНИИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Максимовский А.Ю.[1]

В работе исследованы свойства двух классов конечных автоматов, которые являются обобщениями регистра сдвига с переносом (памятью) (РСП). Данные классы были построены на основе установленного изоморфизма РСП и регистра сдвига над кольцом целых чисел, а также экспоненциального представления выходной последовательности РСП и полученных в работе ранее неизвестных свойств выходных последовательностей РСП. Получены необходимые и достаточные условия существования диагностических и установочных экспериментов для предложенных обобщений РСП, оценки длины этих экспериментов и трудоемкости их реализации, оцениваемую числом операция в соответствующих кольцах. Указанные параметры характеризуют временную и ресурсную сложность процедур контроля за функционированием устройств, математическими моделями которых являются рассматриваемые автоматы. Показано, что эффективность использования операции реверса для решения этих задач существенно зависит от строения колец, над которыми построены эти автоматы. Для одного из классов обобщенных РСП предложен метод нахождения запретов выходных последовательностей, что позволяет расширить как перечень параметров таких устройств, подлежащих мониторингу в процессе их функционирования, так и их функциональность в целях выявления скрытых каналов утечки информации и организации противодействия данным угрозам безопасности информационных систем.

Ключевые слова: *эксперименты с автоматами, запреты автоматов, изоморфизмы и автоморфизмы автоматов, скрытые каналы утечки информации*

DOI: *10.21681/2311-3456-2019-1-69-76*

Под регистром сдвига с переносом (иногда используется термин «с памятью) (РСП) ([1]) будем понимается регистр сдвига, определяемый следующим образом. Пусть $(a_{n-1},...,a_0)$ – заполнение накопителя регистра, m_{n-1} – содержимое памяти регистра в некоторый момент времени, $a_i \in \Omega_p = \{0,1,...,p-1\}$, $i=0,1,...,n-1$, $m_{n-1} \in Z$,. Пара $(m_{n-1}, (a_{n-1},...,a_0))$ является состоянием регистра, параметр n назовем длиной регистра. Из состояния $(m_{n-1}, (a_{n-1},...,a_0))$ регистр переходит в состояние $(m_n, (a_n,...,a_1))$, где $p_{mn} + a_n = m_{n-1} + \sum_{i=1}^{n} q_i a_{n-i}$, $a_n \in \Omega_p$, $q_i \in \Omega_p$, $i=1,...,n$, $q_n \neq 0$. При этом на выход регистра поступает a_0. Число $q = -1 + \sum_{i=1}^{n} q_i p^i$ называется соединительным числом РСП. Определение РСП было введено в научный оборот в 1994 г. Клаппером и Горецки (обзор приведен в [1, 2]), а также независимо от них Марсалья и Заманом [3], Кутюмом и Л'Экуером [4]. При этом первые стремились использовать эту конструкцию для криптоанализа суммирующего генератора, а вторые – для создания «хорошего» генератора псевдослучайных чисел

Отметим, что в работах [5-7] были предложены обобщения РСП на более широкие по сравнению с исходными классы автоматов, тем не менее, рассматриваемые в данной работе обобщения РСП, хотя и имеют пересечения в теоретико-множественном смысле, но опираются на принципиально другие свойства и трукту-ру колец, которые рассматриваются в указанных статьях (см. также [7, 8]). При этом в работах [1-8] вопросы, характерные при изучении автоматов, подробно не рассматривались. Исследованию отдельных теоретико-автоматных свойств и аппаратной реализации регистрами сдвига, в которых существенно использование операции модульного суммирования, посвящены работы [9-11].

1. Изоморфизм РСП и редуцированного регистра сдвига

Пусть t и p – некоторые фиксированные целые числа. Обозначим $R_{t,p}=(S,Y,h,f)$ – автономный автомат, у которого множество состояний S совпадает с множеством целых чисел Z, выходной алфавит $Y=\Omega_p$, функция переходов h определена по правилу:

$h(s)=rt+k$, если $s = kp+r$, $r \in \Omega p$, $k \in Z$. (1)

Функция выходов $f(s)=s \pmod p$. Если $t>0$ и $0 \le s \le pt-1$, то автомат $R_{t,p}$ реализует подстановку редуцированного регистра сдвига $R_{t,p}(e,e)$ (см. [12]) где e – единичная подстановка множества Ω_t. Автомат $R_{t,p}$ будем называть, следуя [12], редуцированным регистром сдвига (РРС). Подстановка РРС $Rt,p(e,e)$ действует на элемент $a \in \Omega_q$: пусть $\gamma p=1 \pmod q$, тогда

а $R_{t,p}(e,e) = \gamma a \pmod q$. $t = \frac{q+1}{p}$

Построим изоморфизм автоматов $R_{t,p}$ при и $R(q)=(S_1,Y,h_1,f_1)$, являющегося автоматной моделью РСП

1 Максимовский Александр Юрьевич, кандидат физико-математических наук, старший научный сотрудник, ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, Россия. E-mail: maximay@ipy.ru

с соединительным числом q. Здесь полагается $S_1=Z\times(\Omega_p)^n$, функция переходов $h_1((m,(a_{n-1},...,a_0)))=(m_1,(a_n,...,a_1))$, где $pm_1+a_n=m+\sum_{i=1}^{n} q_i a_{n-i}$, и функция выходов $f_1((m,(a_{n-1},..., a_0)))=a_0$.

Покажем, что отображение $\varphi:S_1\to S$, задаваемое равенством

$$\phi((m,(a_{n-1},\dots,a_0)))= mp^n - \sum_{k=0}^{n-1} p^k \sum_{i=0}^{k} q_i a_{k-i} \quad (2)$$

где $q_0=-1$, является биективным. Действительно, если имеет место равенство $\varphi((m,(a_{n-1},...,a_0))) = \varphi((s,(b_{n-1},...,b_0))$ для $(m,(a_{n-1},...,a_0))$ и $(s,(b_{n-1},...,b_0))$, то

$$mp^n - \sum_{k=0}^{n-1} p^k \sum_{i=0}^{k} q_i a_{k-i} = sp^n - \sum_{k=0}^{n-1} p^k \sum_{i=0}^{k} q_i b_{k-i} \quad (3)$$

Из (3), в частности, следует, что число $q_0(a_0-b_0)$ делится на p, и потому $a_0=b_0$. Пусть $a_j=b_j$, $j\in\{0,...,k-1\}$. Тогда число

$$c_k= \sum_{i=0}^{k} q_i a_{k-i} - \sum_{i=0}^{k} q_i b_{k-i}$$

– делится на p. Поскольку $a_j=b_j$, $j\in\{0,...,k-1\}$, $c_k=q_0(a_k-b_k)$. Следовательно, $a_j=b_j$, $j\in\{0,...,n-1\}$, и из (2) получаем, что m=s. Поэтому отображение φ биективно.

Пусть автомат $R(q)$ переходит из состояния $(m_{n-1},(a_{n-1},...,a_0))$ в состояние $(m_n,(a_n,...,a_1))$, при этом $pm_n+a_n=m_{n-1}+\sum_{i=1}^{n} q_i a_{n-i}$. Введем обозначения

$$s_{n-1}= m_{n-1}p^n - \sum_{k=0}^{n-1} p^k \sum_{i=0}^{k} q_i a_{k-i}\,,\quad s_n= m_n p^n - \sum_{k=0}^{n-1} p^k \sum_{i=0}^{k} q_i a_{k-i+1}\,,$$

Покажем, что автомат $R_{\frac{q+1}{p},p}$ переходит из состояния s_{n-1} в состояние s_n.

Действительно, $s_{n-1}=(m_{n-1}p^{n-1}- \sum_{k=1}^{n-1} p^{k-1} \sum_{i=0}^{k} q_i a_{k-i})p+a_0$.

Тогда

$$h(s_{n-1}) = a_0\frac{q+1}{p} + m_{n-1}p^{n-1} - \sum_{k=1}^{n-1} p^{k-1} \sum_{i=0}^{k} q_i a_{k-i} =$$

$$= a_0 \sum_{i=1}^{n} q_i p^{i-1} + (pm_n+a_n- \sum_{i=1}^{n} q_i a_{n-i})p^{n-1} - \sum_{k=1}^{n-1} p^{k-1} \sum_{i=0}^{k} q_i a_{k-i} =$$

$$= m_n p^n - \sum_{k=0}^{n-1} p^k \sum_{i=0}^{k} q_i a_{k-i+1} = s_n.$$

Поэтому пара отображений (φ,ε), где ε – тождественное преобразование множества Y, задает изоморфизм $R_{\frac{q+1}{p},p}$ автоматов $R(q)$ и $R_{\frac{q+1}{p},p}$.

Таким образом, доказано

Утверждение 1. Автомат R(q), соответствующий p-ичному РСП с соединительным числом q, изоморфен $R_{\frac{q+1}{p},p}$ и эквивалентен автомату $R_{\frac{q+1}{p},p}$.

Полученный результат позволяет получить ряд результатов о свойствах РСП без привлечения аппарата p-адических чисел, опираясь на свойства редуцированного регистра сдвига (см. [12, 15]). Приведем эти результаты как следствия из утверждения 1.

Следствие 1. Периодическими состояниями автомата $R(q)$ являются состояния вида $\varphi^{-1}(s)$, $0\le s\le q+1$, и только они. Состояния $(1,(0,...,0))$ и $(0,(1,0,...,0))$ являются периодическими при любых q и p.

Следствие 2. Число неединичных циклов отображения h_1 и их длина совпадают с числом неединичных циклов и их длиной подстановки ρ кольца Z_q вычетов по модулю q, определяемой равенством $z^{\rho}=pz\ (mod\ q)$.

Следствие 3. Число единичных циклов отображения h_1 равно $d+1$, где d – наибольший общий делитель чисел $p-1$ и $\frac{q-p+1}{p}$.

Поэтому при $p>2$ число q целесообразно выбирать таким, чтобы числа $p-1$ и $\frac{q-p+1}{p}$ были взаимно простыми. Следствие 3 показывает, что при переходе от $p=2$ к $p>2$ появляются новые свойства, которые могут оказать существенное влияние на свойства РСП.

Следствие 4. РСП не имеет эквивалентных состояний.

Следствие 5. Для любых $b_i\in\Omega_p$, $i=1,...,n$, существует периодическое состояние s автомата $R=R(q)$ такое, что выходная последовательность инициального автомата R_s содержит n-грамму $(b_1,...,b_n)$.

При практической реализации РСП размер памяти естественно будет ограничен. В связи с этим возникает вопрос о длине подхода к циклу отображения h_1 множества $S_{1,w}=\Omega_w\times(\Omega_p)^n$. С помощью утверждения 1 мы можем получить достижимую оценку длины подхода к циклу отображения $h_{1,w}$ множества $S_{1,w}$ на себя, являющегося ограничением отображения h_1 на множестве $S_{1,w}$.

Утверждение 2. Длина подхода к циклу отображения $h_{1,w}$ не превосходит величины $n+\log_p(w-p)$.

Доказательство. Рассмотрим преобразование r множества $\varphi(S_{1,w})$, определяемое равенством $r(s)=h(s)$ для всех $s\in\varphi(S_{1,w})$. Очевидно, длина подхода к циклу преобразования r равна длине подхода к циклу отображения $h_{1,w}$. Пусть s – «висячая» вершина графа преобразования r. Если $s<0$, то $s>q-(w-1)p^n$, и потому длина подхода не превосходит $n+\log_p(w-p)$ и может достигнуть этой величины при $s=-(w-p)p^{n-2}$. Если $s>0$, то $s<wp^n$, и максимум длины подхода к циклу достигается при таком s, что $r^k(s)$ не делится на p при всех k, $0<k<t$, где t – минимальное со свойством: $r^t(s)$ – циклическая вершина. Несложно подсчитать, что в этом случае $t\le n-\log_p\frac{q}{pw}$. Утверждение доказано.

Утверждение 3. Если число p является примитивным корнем по модулю q, то группа автоморфизмов автомата $R(q)$ имеет порядок два.

Доказательство. Согласно утверждению 1 для описания автоморфизмов РСП достаточно описать автоморфизмы изоморфного ему РРС.

Автоморфизмами автомата $R_{t,p}$ являются пары отображений $(\varepsilon_S,\varepsilon_Y)$, где ε_S и ε_Y – тождественные отображения множества состояний и выходного алфавита соответственно, и (ψ_S, φ_Y), где $\psi_S(s)=tp-1-s$, $\varphi Y(y)=p-1-y$. Действительно, если $s = kp+r$, $r\in\Omega_p$, $k\in Z$, то имеют место равенства

$h(\psi_S(s))=h(tp-1-s)=h((t-k-1)p+p-r-1)=(p-r-1)t+t-k-1=$

$=tp-1-(tr+k)=tp-1-h(s)=\psi_S(h(s))$.

При этом, очевидно, $\varphi_Y(f(s))=f(\psi_S(s))$.

Пусть число p является примитивным корнем по модулю q. Тогда функция переходов h индуцирует подстановку $R_{t,p}(e,e)$ на множестве Ω_{q+1}, которая имеет два единичных цикла и цикл длины $q-1$. Поэтому отображение ψ множества состояний при любом автоморфизме (ψ,φ) автомата $R(q)$ переставляет между собой эти два единичных цикла и централизует «длинный» цикл.

Поскольку централизаторы подстановок $R_{t,p}(e,e)$ и $\chi=R_{t,p}(e,e)^{-1}$ совпадают, то для удобства далее будем рассматривать только централизатор подстановки χ. Подстановка χ действует на множестве Ω_q следующим образом: $a\chi=pa \pmod q$, $a\in\Omega_q$. Поскольку p является примитивным корнем по модулю q, то любой ненулевой элемент $a\in\Omega_q$ имеет вид $a=p^i \pmod q$ для некоторого i. Поэтому отображение ψ переводит элемент $a=p^i \pmod q$ в элемент $b=p^{i+j} \pmod q$ для некоторого фиксированного j.

Рассмотрим два случая.

1. Если $0\psi=0$, то $q\psi=q$, $0\varphi=0$, $(p-1)\varphi=p-1$. Поэтому

$(p^{i+1} \bmod q) \pmod p = 0$,

$((p-1)p^i \bmod q) \pmod p = p-1$.

Из первого равенства следует, что $p^{i+1}=l_jp+kq$ для некоторых l_j и k. Тогда p делит kq, и в силу взаимной простоты p и q получаем, что p делит k. Пусть $k=pk'$. Тогда $(p-1)p^i=(k-k')q+l_j(p-1)$. Следовательно, $(p-1)p^i\equiv l_j(p-1) \pmod q$, и с учетом того, что $(l_j(p-1) \bmod q) \pmod p = p-1$, получаем что $l_j = 1 \pmod p$. Поскольку $p^i=l_j+k'q$, то $(p^i \bmod q) \pmod p = 1$, и потому $1\varphi=1$. Следовательно, $(p-2)\varphi=p-2$, так как существует автоморфизм $(\psi S, \varphi Y)$.

Обозначим через v минимальное число со свойством: $(v-1)l_j<q$, $vl_j\geq q$. Тогда для любого $i<v$ имеют место равенства $(l_ji \bmod q) \pmod p = i$, $i\varphi=i$, $(p-i)\varphi=p-i$. В то же время $(l_jv \bmod q) \pmod p = v+1$, поскольку $l_jv \equiv l_jv - q \pmod q$, $q=p-1 \pmod p$, и мы приходим к противоречию с биективностью отображения φ. Следовательно, отображение φ – тождественное. Тогда отображение ψ действует на последовательностях состояний, соответствующих n-граммам вида $(b,b,...,b)$, как тождественное, поэтому $j=0$, и отображение ψ - тождественное.

Таким образом, в случае 1 автоморфизм (ψ,φ) совпадает с $(\varepsilon S,\varepsilon Y)$.

2. Если $0\psi=q$, то $q\psi=0$, $0\varphi=(p-1)$, $(p-1)\varphi=0$. При автоморфизме автомата $R(q)$, являющегося композицией автоморфизмов $(\psi S,\varphi Y)$ и (ψ,φ), состояние 0 остается на месте. Такой автоморфизм удовлетворяет условиям случая 1, и потому является тождественным. Поскольку отображения ψS и φY – инволюции, то $(\psi S,\varphi Y) = (\psi,\varphi)$.

Следовательно, в условиях утверждения группа автоморфизмов РСП имеет порядок два.

Заметим, что даже в случае $p>2$ группа автоморфизмов РСП имеет определенные сходства с группой автоморфизмов 2-адического регистра сдвига, описанной в [13].

Сформулируем еще два очевидных следствия

Следствие 6. При любых p и q РСП имеет нетривиальный автоморфизм, при котором состояние $(m_{n-1}, (a_{n-1}, ...,a_0))$ переходит в состояние $(w-m_{n-1}, (p-1-a_{n-1},...p-1-,a_0))$, где $w= q_n+...+q_1$.

Следствие 7. Если последовательность $b=\{b(i)\}$ является выходной последовательностью РСП для некоторого начального состояния, то существует такое начальное состояние РСП, что соответствующая выходная последовательность имеет вид $\{p-1-b(i)\}$.

Следствие 7 позволяет сделать вывод о возможности построения диагностических экспериментов ([14]) для РСП, используя выявленный дуализм выходных последовательностей.

2. Свойства обобщенных РСП

2.1. Рассмотрим обобщение РСП в виде регистра сдвига специального вида над конечным кольцом. Следует пояснить, что потенциально множество состояний РСП бесконечно, однако множество циклических состояний у него всегда конечно, и потому предлагаемое ниже обобщение содержательно.

Пусть C – конечное кольцо, n – элемент, который не обратим в кольце C. причем идеал ${}_nC$ ненулевой. Пусть $C=(nC+c_0)\bigcup({}_nC+c_1)\bigcup...\bigcup({}_nC+c_{s-1})$, где $c_0, c_1,..., c_{s-1}$ – фиксированные представители смежных классов, $c_0\bigcup{}_nC$, – разложение кольца C в смежные классы по идеалу ${}_nC$. Определим преобразование σ кольца C следующим образом:

$c\sigma =nc + \lambda(c)$,

где λ – отображение кольца C на множество $\{c_0, c_1,..., c_{s-1}\}$.

Определим функцию $\psi:C\to\Omega_s=\{0,...,s-1\}$ по правилу: $\psi(c)=i$, если $c\in nC+c_i$. Легко видеть, что $\psi(c\sigma)=\psi(\lambda(c))$, поэтому функцию ψ можно рассматривать как аналог модульной функции.

Введенные обозначения позволяют определить автономный автомат $B=(C, \Omega_s, \sigma, \psi)$, для которого мы исследуем ниже вопросы построения диагностических и установочных экспериментов (см. [14]), а также характерные свойства его выходных последовательностей. Автомат B в случае $C=Z_{nm}$, $ci=i$, $\lambda(c)=d$, если $c=dm+r$, $r\in\Omega_m$, реализует подстановку редуцированного регистра сдвига (см. [12,15]) и вопрос о построении диагностических и установочных экспериментов решается относительно просто с учетом результатов [12, 15].

Найдем условия, при которых преобразование σ является подстановкой кольца C. Обозначим ${}_nD$ множество правых аннуляторов элемента n, то есть ${}_nD=\{c\in C \mid nc=0\}$. Очевидно, ${}_nD$ является правым идеалом кольца C.

Утверждение 4. Преобразование σ является подстановкой кольца C тогда и только тогда, когда для любых элементов c, c´ кольца C, сравнимых по модулю идеала ${}_nD$, выполнено условие $\lambda(c)\neq\lambda(c')$.

Доказательство. Предположим, что преобразование σ не является подстановкой кольца C. В силу конеч-

ности кольца C это предположение эквивалентно условию: для некоторых элементов c, c´ кольца C выполнено равенство

$nc + \lambda(c) = nc' + \lambda(c')$.

Тогда элемент $\lambda(c) - \lambda(c') \in {}_nC$. Поэтому $\lambda(c) = \lambda(c')$. Следовательно, элемент $(c \quad c') \in {}_nD$. Утверждение доказано.

Следствие 8. Если преобразование σ является подстановкой кольца C, то ограничение отображения λ на любом смежном классе кольца C по идеалу ${}_nD$ является биекцией.

Доказательство. Очевидно, порядок идеала ${}_nD$ равен индексу $[C:nC]$ подгруппы ${}_nC$ в аддитивной группе C. Отсюда по утверждению 1 получаем требуемое.

Обозначим $\Lambda_и=\{c \in C \mid \lambda(c)=и\}$. Тогда для любых a, $c \in \Lambda_и$ разность $(c\sigma - a\sigma)$ сравнима по модулю ${}_nC$. Следовательно, $\psi(c\sigma) - \psi(a\sigma) = 0$. Таким образом, одинаковые символы в выходной последовательности автомата B указывают на состояния автомата, относящиеся к одному и тому же множеству $\Lambda_и$. Данная информация является крайне важной при проведении установочного эксперимента с автоматом B. Она указывает, с одной стороны, на возможную неоднозначность результата эксперимента при попытке «лобового» решения задачи, и, с другой стороны, на целесообразность введения применительно к эксперименту с автоматом B дополнительной характеристики – трудоемкости его реализации.

Следствие 9. *Если преобразование σ является подстановкой, то ни одна пара элементов множества $\Lambda_и$ не принадлежит одному и тому же смежному классу кольца C по идеалу ${}_nD$.*

Запишем закон функционирования автомата B в следующем виде:

$$x_{i+1}=x_i\sigma,\ i=0,1,\ldots,m-1, \qquad (4)$$
$$y_i=\psi(x_i),\ i=0,1,\ldots,m-1.$$

Обозначим $c_{y(i)}=\psi^{-1}(yi)$. Тогда в соответствии с (4) состояние $x_i \in nC+c_{y(i)}$. Следовательно, $x_{i+1} \in n^2C+nc_{y(i)}+c_{y(i+1)}$. При этом представитель смежного класса кольца C по идеалу n^2C нам известен. Отсюда следует, что

$$x_{i+l} \in n^{l+1}C+\sum_{j=0}^{l-1} n^{l-j}c_{y(i+j)},$$

где $n^0c_{y(i+l)}$ обозначает $c_{y(i+l)}$.

Таким образом, мы можем определить состояние x_{i+l} автомата B с точностью до смежного класса кольца C по идеалу $n^{l+1}C$, представитель которого нам известен. Поскольку n – необратимый элемент кольца C, то существует такое натуральное $l(n)$, что $n^{l(n)+i}C=n^iC$ для всех i, больших некоторого $i(n)$.

Обозначим $m(n)$ минимальное натуральное число со свойством: мощность $n^{m(n)}C$ минимальна. Тогда для состояния $x_{m(n)}$ мы получим минимальное число вариантов. Перебирая эти варианты, мы сможем определить состояние $x_{m(n)}$ автомата B Если преобразование σ является подстановкой, то мы сможем затем восстановить и начальное состояние x_0, и тем самым решить задачу диагностического эксперимента для автомат B.

Оценим длину предложенного установочного эксперимента для автомата B. Для построения множества возможных вариантов состояния $x_{m(n)}$ требуется $m(n)-1$ выходных символов. Кроме того, необходимо не менее $\log_s |n^{m(n)}C|$ выходных символов для вычисления истинного значения состояния $x_{m(n)}$. Таким образом, доказано

Утверждение 5. Существует установочный эксперимент для автомата B. трудоемкость которого оценивается величиной $O(|n^{m(n)}C|)$. При этом длина указанного эксперимента не превышает величины

$$\log_s |n^{m(n)}C \cap \Lambda_{u(m(n))}|+m(n)-1.$$

Следствие 10. Если преобразование σ является подстановкой, то установочный эксперимент для автомата B является также диагностическим.

Результат утверждения 3 и следствия 3 показывают, что эффективность предложенного метода построения установочного (и диагностического) эксперимента автомата B существенно зависит от мощности идеала $n^{m(n)}C$. Очевидно, что метод наиболее эффективен, если элемент n является нильпотентным $(n^{m(i)}=0)$, и наименее эффективным, если элемент n является идемпотентом $(n^2=n)$.

Для повышения эффективности метода воспользуемся включением $x_i \in \Lambda_{и(i)}$, если $y_{i+1}=\psi(и(i))$. Действительно, в рассматриваемом случае оказывается, что для любого $i \geq 0$ $x_i \in (nC+c_{y(i)}) \cap \Lambda_{и(i)}$. Это условие может оказаться наиболее полезным в случае, когда преобразование σ является подстановкой, поскольку следствие 2 устанавливает достаточно узкие ограничения на вид элементов множества $(nC+c_{y(i)}) \cap \Lambda_{и(i)}$. На основании этих рассуждений и с учетом утверждения 2 мы можем сформулировать

Утверждение 6. Для автомата B существует установочный эксперимент длиною не более $\log_s |n^{m(n)}C \cap \Lambda_{u(m(n))}|+m(n)-1$ и трудоемкостью порядка $O(|n^{m(n)}C \cap \Lambda_{u(m(n))}|)$.

Замечание 1. Использование реверса автомата в некоторых случаях позволяет упростить задачу построения экспериментов (особенно диагностических), исследуем свойства преобразование σ^{-1} в случае, когда преобразование σ является подстановкой.

Согласно утверждению 4 преобразование σ^{-1} можно представить в следующем виде. Если $c=nc_1+c_2$, то $c\sigma^{-1}=d_0+c_1$, где $d_0 \in {}_nD$, c^1 - представитель смежного класса по идеалу ${}_nD$, $c_2=\lambda(d_0+c_1)$. Следовательно, $c\sigma^{-1}$ определяет элемент, по которому «пересекаются» множества ${}_nD+c_1$ и $\lambda^{-1}(c_2)$. Полученное представление показывает, что в случае, когда кольцо C произвольно, использование реверса может не принести существенного упрощения исходной задачи.

2.2. Рассмотрим теперь свойства другого обобщения РСП, основанного на экспоненциальном представлении выходной последовательности РСП. Определим автомат $A=(C, \Omega s, \rho, \psi)$ следующим образом. Пусть K, C – конечные кольца с единицей, причем K – подмножество C, n – элемент, который обратим в кольце K и не обратим в кольце C. Определим преобразование (подстановку) ρ кольца C следующим образом:

$c\rho=nc$, если $c\in K$,

при этом операция умножения выполняется в кольце K,

$c\rho=c$, если $c\in C\setminus K$.

Функция $\psi: C\to\Omega_s$ определена по правилу: $\psi(c)=i$, если $c\in {}_nC+c_i$, где где $c_0=0$, $c_1,\ldots,c_{s-1}$ – фиксированные представители смежных классов кольца C в по идеалу ${}_nC$, который в отличие от определения автомата В может быть нулевым.

Исследуем свойства выходной последовательности $\underline{y}=\psi(x_1),\ldots,\psi(x_l)$, автомата A, где $x_1,\ldots,x_l$ – последовательность его состояний. Естественно предположить, что последовательности $\underline{y}$ принадлежат хотя бы два различных элемента множества Ω_s, поскольку в противном случае функционирование автомата A не имеет смысла.

В отличие от функции переходов автомата B функция переходов автомата A всегда является подстановкой, поэтому определение некоторого состояния автомата A равносильно определению начального состояния этого автомата. Используя регулярность автомата A, можно предложить метод восстановления начального состояния этого автомата, который является модификацией предложенного выше метода применительно к реверсу автомата A.

Приведем пример ситуации, в которой выходная последовательность автомата A состоит из единственного элемента. Пусть C – кольцо матриц размера 2×2 над произвольным конечным полем P, K – множество всех матриц, которые имеют вид $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, где a – произвольный элемент поля P. В качестве элемента n выберем элемент $\begin{pmatrix} \theta & 0 \\ 0 & 0 \end{pmatrix}$, где θ - примитивный элемент поля P. Идеал nC состоит из всех матриц вида $\begin{pmatrix} b & g \\ 0 & 0 \end{pmatrix}$, $b, g \in P$. Очевидно, $K\subseteq {}_nC$, и потому выходная последовательность автомата A состоит из одних нулей.

Выходную последовательность автомата A, имеющую период 1, будем называть вырожденной. Заметим, что если начальное состояние автомата A не принадлежит кольцу K, то выходная последовательность будет вырожденной. Назовем автомат A вырожденным, если его выходная последовательность является вырожденной независимо от начального состояния.

Приведенный пример позволяет сформулировать необходимое условие невырожденности автомата A.

Утверждение 7. Если автомат A не является вырожденным, то множество K имеет непустые пересечения не менее, чем с двумя различными смежными классами кольца C по идеалу ${}_nC$.

Условие, сформулированное в утверждении 4, не является достаточным. Действительно, если последовательность состояний $\{x_i, i=1, 2, \ldots\} = \{n^j x_1, j=0, 1, \ldots\}$, где $n^0x_1=x_1$, начиная с некоторого t, полностью содержится в некотором смежном классе кольца C по идеалу ${}_nC$, то выходная последовательность автомата A будет вырожденной.

Проведенные выше рассуждения позволяют сделать вывод, что в случае, когда последовательность $\underline{y}=\psi(x_1),\ldots,\psi(x_l)$ является невырожденной, состояние $x_i\in K$ для любого $i\geq 1$. Всюду далее будем считать последовательность $\psi(x_1),\ldots,\psi(x_l)$ невырожденной.

Обозначим $K_j=K\cap({}_nC+c_j)$, $(ab)_K$ – результат умножения элементов a и b кольца K. Очевидно, $x_i\in K_{\psi(x_i)}$, $i=1,\ldots,l$. При этом $(nx_i)_K=x_{i+1}\in K_{\psi(x_i)}$. Рассмотрим разбиение

$$ {}^nK_i = K_{i,0}\cup\ldots\cup K_{i,s-1}, \qquad (5)$$

где $K_{i,j} = {}_nK_i\cap({}_nC+c_j)$, причем в (5) при вычислении элементов множества ${}_nK_i\subseteq K$ операции проводятся в кольце K. В частности, $x_{i+1}=(nx_i)_K\in K_{\psi(x_i),\psi(x_{i+1})}$.

Разбиение (5) можно продолжить следующим образом

$$K_{i_1,\ldots,i_t} = nK_{i_1,\ldots,i_{t-1}}\cap(nC+c_{i_t}),\ t>1.$$

При этом $x_j\in K_{\psi(x_i),\psi(x_{i+1})}$. Отсюда мы получаем достаточное условие существования диагностического эксперимента для автомата A.

Утверждение 8. Если для некоторого $t>0$ мощность множества $K_{i_1,\ldots,i_t}$ равна единице для любых $i_1,\ldots,i_t$, то существует диагностический эксперимент для автомата A длины t.

Замечание 2. В условиях утверждения 8 последовательность $\psi(x_1),\ldots,\psi(x_t)$ является «сильным» установочным экспериментом для автомата A в том смысле, что она позволяет однозначно определить каждое состояние $x_j\in K_{\psi(x_1),\ldots,\psi(x_j)}$. При этом для нахождения состояния xt автомата A необходимо или построить множества $K_{i_1,\ldots,i_t}$ для всех реализуемых наборов выходных символов $i_1,\ldots,i_t$, где $i_j\in\Omega_s$, $j=1,\ldots,t$, и тогда состояние xt можно определять по построенному каталогу, или последовательно строить множества $K_{\psi(x_1)}$, $K_{\psi(x_1),\psi(x_2)}$, $K_{\psi(x_1),\ldots,\psi(x_t)}$ постоянно сужая множества состояний, рассматриваемых на каждом шаге.

Первый вариант обсуждаемого метода определения состояния автомата A имеет довольно большую трудоемкость (порядка $t|K|$ операций в кольцах C и K), и потому не представляет значительного интереса. Трудоемкость второго варианта метода можно оценить сверху величиной $t|K_{\psi(x_1)}|$ операций в кольцах C и K. Поэтому второй вариант метода можно считать удовлетворительным, если будут выполнены два связанных между собой условия:

1. Параметр t относительно мал.

2. Мощность множества $K_{\psi(x_1),\ldots,\psi(x_t)}$ убывает «быстро» с ростом длины выходной последовательности.

Если эти условия не будут выполнены, то и второй вариант метода может оказаться также достаточно трудоемким.

Замечание 3. Оценка, приведенная в утверждении 5, может быть значительно улучшена для конкретных классов колец. Например, если кольца K и C являются кольцами вычетов по различным модулям, то трудоемкость второго варианта метода не превышает $|K_{\psi(x_1)}|$

операций в кольцах C и K, а величина параметра t не превышает $log_s|K_{\psi(x_1)}|+1$.

Действительно, пусть кольца K и C являются кольцами вычетов по различным модулям – k и r, соответственно. При этом идеал ${}_nC$ совпадает с идеалом ${}_dC$, где $d=(n,r)$ – наибольшему общему делителю чисел n и r, $d>1$, а параметр $s=d$.

В связи с этим, уместно поставить вопрос о минимизации рассматриваемой конструкции автомата A с точки зрения мощности кольца C. Действительно, если C' - подмножество кольца C, которое само является кольцом, содержит кольцо K, причем элемент n кольца K не является обратимым элементом кольца C', и индекс идеала nC' в кольце C' равен индексу идеала nC в кольце C, то уместно рассматривать автомат A над кольцом C'. При этом, если окажется, что $({}_nC'+c'_j) \subseteq ({}_nC+c_j)$, где $j=0,...,s-1$, $c'_0,..., c'_{s-1}$ – представители соответствующих смежных классов кольца C′ по идеалу ${}_nC'$, то автомат A над кольцом C' эквивалентен автомату A над кольцом C. Примером отмеченной эквивалентности способов задания автомата A является автомат A, в определении которого кольцо $K=Z_k$, $C=Z_r$, $(k,r)=1$, $(n,r)=2$, $r-k>3$, $C'=Z_{r-2}$.

Поскольку при определении функций переходов и (как следствие) выходов автомата A используются мультипликативное операции в соответствующих кольцах, то представляет определенный интерес исследование линейных соотношений, связывающих состояния автомата A, для поиска линейных связей для выходных последовательностях. По существу, это вопрос о возможности сведения автомата A к линейному регистру сдвига над кольцом K с выходной функцией ψ (см. [16-19])

Пусть $k_1,..., k_q$ – набор элементов кольца K таких, что

$$\left(\sum_{i=1}^{q} k_i n^i\right)_K = 0 .$$

Тогда состояния $x_1,..., x_{q+1}$ автомата A удовлетворяют равенству

$$\left(\sum_{i=1}^{q} k_i x_{i+1}\right)_K = 0 . \quad (6)$$

Если для набора символов $i_1,...,i_q$, $i_j \in \Omega_s$, $j=1,...,q$, не существует таких элементов $x_1,..., x_{q+1}$ кольца K, что $x_{j+1}=(nx_j)_K$, и $x_{j+1} \in Ki_j$, $j=1,...,q$, то набор $i_1,...,i_q$ не может появиться в выходной последовательности автомата A. Такой набор, следуя [20-23], будем называть запретом для выходной последовательности автомата A.

Наличие запретов существенно и, как правило, отрицательно влияет на свойства автомата в том числе с точки зрения их защищенности от внешних воздействий. Поэтому актуальна задача построения алгоритмов поиска запретов в том числе в целях описания выходных последовательностей, появление которых будет однозначно указывать на аварийное поведение объета защиты или наличие в нем недокументированных возможностей (см. [24],).

Для поиска запретов автомата A предлагается следующая процедура. Если нам известны значения $\psi(x_2),..., \psi(x_{q+1})$, то мы можем вычислить подмножества $k_j K_{\psi(x_{j+1})}$, $j=1,...,q$, кольца K, которым принадлежат слагаемые в левой части равенства (6). Следовательно, если выбрать такие $i_1,...,i_q$, $i_j \in \Omega_s$, $j=1,...,q$, что для элементов $x_{j+1} \in KI_j$, $zj \in kj\ Kij=1,...,q$, равенства

$$\left(\sum_{j=1}^{q} z_j\right)_K = 0, \quad (7)$$

$$z_j=K_jX_{j+1},\ j=1,...,\ q, \quad (8)$$

$$x_{j+1}=(nx_j)_K,\ j=1,...,q, \quad (9)$$

одновременно не могут иметь места, то $i_1,...,i_q$ – запрет для выходной последовательности автомата A.

Отметим, что очень часто для построения запрета оказывается достаточным проверить только равенство (7) для всех $z_j \in k_j K_{i_j}$, $j=1,...,q$

Вместе с тем, результаты исследования запретов рассматриваемого обобщения РСП, показывают, что если множества $k_j K_{i_j}$, $j=1,...,q$, имеют небольшую мощность, то трудоемкость проверки равенств (7) – (9), с одной стороны, будет относительно небольшой, а с другой стороны, выполнимость равенства (7) для произвольного набора $i_1,...,i_q$, $i_j \in \Omega_s$, $j=1,...,q$, будет проблематичной.

Используя регулярность автомата A, можно предложить способ построения диагностического эксперимента для этого автомата, который является модификацией метода, предложенного в разделе 2.1. Обозначим m – левый обратный элемент к элементу n в кольце K. Тогда мы можем рассмотреть автомат $A'=(C, \Omega_s, \rho', \psi)$, определяемый следующим образом:

$c\rho'=mc$, если $c \in K$,

при этом операция умножения выполняется в кольце K,

$c\rho'=c$, если $c \in C \setminus K$.

Функция $\psi: C \to \Omega_s$ определена так же, как и выше. Независимо от того, является или не является m обратимым элементом кольца C, мы можем по аналогии с (2) рассмотреть разбиения вида

$$R_{i_1,...,i_{t-1}} = R_{i_1,...,i_{t-1},0} \cup ... \cup R_{i_1,...,i_{t-1},s-1},$$

где

$$R_{i_1,...,i_t} = mR_{i_1,...,i_{t-1}} \cap (nC + c_{i_t}),\ t>1.$$

При этом $K_j=R_j$, и, очевидно, $x_j \in R_{\psi(x_t),...,\psi(x_j)}$.

К реверсу автомата A мы можем применить построенные выше способы построения диагностических (установочных) экспериментов, а также поиска запретов. Выигрыш от использования реверса может быть достигнут за счет простоты вычисления результатов операций в кольце K. В частности, несложно заметить, что использование реверса двоичного РСП значительно упрощает вычисления.

Заключение

Полученные результаты показывают эффективность использования изоморфизма на редуцированные ре-

гистр сдвига при исследовании периодических свойств, построения диагностических и установочных экспериментов с классом автоматов, который включает p-ичные РСП. В частности, выявлены ранее неизвестных свойств выходных последовательностей указанных РСП.

Это послужило стимулом к определению и исследованию свойств двух классов конечных автоматов, которые являются обобщениями РСП. Данные классы были построены на основе редуцированного регистра сдвига над кольцом целых чисел, а также экспоненциального представления выходной последовательности РСП. При этом объекты и проблематика исследований не пересекались с известными обобщениями РСП.

В результате исследований:

1. Получены необходимые и достаточные условия существования диагностических и установочных экспериментов для предложенных обобщений РСП.

2. Найдены верхние оценки длины этих экспериментов и трудоемкости их реализации, оцениваемую числом операция в соответствующих кольцах.

3. Проведен анализ эффективности использования операции реверса этих для снижения временной и ресурсной сложности процедур контроля за функционированием устройств, математическими моделями которых являются рассматриваемые автоматы. Оказалось, что эффективность использования операции реверса для решения этих задач существенно зависит от строения колец, над которыми построены эти автоматы.

4. Для одного из классов обобщенных РСП предложены методы построения линейных соотношений и поиска запретов выходных последовательностей. Это позволяет расширить как перечень параметров таких устройств, подлежащих мониторингу в процессе их функционирования, так и их функциональность в целях выявления скрытых каналов утечки информации и организации противодействия данным угрозам безопасности информационных систем.

Литература:

1. A.Klapper, M.Goresky. Feedback Shift Registers, 2-Adic Span, and Combiners with Memory. J.Cryptology, 1997, v.10, N 2, pp. 111-147.
2. A.Klapper, M.Goresky. Feedback Shift Registers, 2-Adic Shift Registers. Fast Software Encryption // Lectures Notes in Computer Science. 1994. V.809, Springer Verlag, N. Y. , pp. 174-178.
3. Marsaglia G. Zaman A. A New Class of Random number Generators // Ann. Appl. Prob., 1991, 1, pp. 462-480.
4. Couture R., L'Ecuyer. On the Lattice Structure of Certain Linear Congruential Sequences Related to AWE/SWB Generatjr // Mathemftics for Computation. 1994, Vol. 62, N. 206, pp. 799-808
5. A.Klapper, Jinzhong Xu. Algibraic Feedback Shift Registers. Theoretical computer Science. 1999. 226, pp. 61-92.
6. A.Klapper, Jinzhong Xu. Register Synthesis for Algibraic Feedback Shift Registers. Design, Codes and Cryptography. 2004. 31(3), pp. 227-250.
7. A.Klapper, M.Goresky. Algabraic Shift Register Sequences. Cambridge University Press. 2012, 514 p.
8. Шрейер Брюс. Прикладная криптография. Протоколы, алгоритмы и тексты на языке С. – Вильямс, 2016. – 1024 с.
9. Песошин В.А., Кузнецов В.М., Гумиров А.И. Генераторы псевдослучайных последовательностей немаксимальной длины на основе регистра с внутренними сумматорами по модулю два (часть 1) // Вестник Чувашского университета. 2017. № 1. С. 263-272.
10. Chen W.-K. The VLSI Handbook, Second Edition. - CRC Press. - Chicago. 2006. – 2320 p.
11. Гришкин А.С. Генераторы псевдослучайных символов на регистрах сдвига с внутренними сумматорами по модулю два при использовании инверсных выходов // Дис. ... к.т.н., 05.13.05 – Элементы и устройства вычислительной техники и систем управления, Казань, КГТУ, 2006, 142 с.
12. Максимовский А.Ю., Мельников С.Ю. Спектральные и комбинаторные свойства редуцированных графов Де Брейна // Вопросы кибербезопасности. 2018. № 4. С. 70-76. DOI: 10.21681/2311-3456-2018-4-70-76.
13. Liu M. Homomorphisms and automorphisms of 2-D de Bruijn-Good graphs // Discrete Mathematics, Vol.85, I.1, 1990, pp. 105-109.
14. Гилл А. Введение в теорию конечных автоматов. М Наука, 1966, 272с.
15. Максимовский А.Ю. О групповых свойствах подстановок, определенных на смежных классах конечной абелевой группы составного порядка по ее подгруппам. Математические вопросы криптографии., 2016, Т.7, № 1, С. 83-92 .
16. Гилл А. Линейные последовательностные машины М. Наука, 1974, 288с.
17. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х томах; Т. 2 – М. Мир. – 822с.
18. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М: Книга по требованию, 2013. 566 с.
19. Камловский О.В. Кузьмин А.С. Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа // Фундамент. и прикл. матем. – 2000. –Т. 6, вып.4, – С.1083–1094.
20. Сумароков С. Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикл. и пром. мат. - 1994. - Т.1 – Вып. 1, С. 33-55.
21. Бабаш А. В. Запреты автоматов и двоичных функций // Труды по дискретной математике. 2006, том 9, С.7–20
22. Бабаш А. В. Запреты автоматов // Математические заметки. 2012, том 91, выпуск 5. С. 667–673.
23. Пархоменко Д.В. Гистограммная функция автомата и ее приложения // Дис. ... к.ф.-м.н. 01.01.09 - Дискретная математика и математическая кибернетика, Москва: МГУ, 2015. – 86 с.
24. Грушо А.А., Грушо Н.А., Тимонина Е.Е. Включение новых запретов в случайные последовательности // Информ. и ее примен., 8:4 (2014), С. 46-52

Рецензент: *Калашников Андрей Олегович, доктор технических наук, заместитель директора ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, Россия. E-mail: tigrilla1962@mail.ru*

ON TWO CLASSES OF AUTOMATA OVER FINITE RINGS, BASED ON THE ISOMORPHISM OF THE SHIFT REGISTER, AND THEIR APPLICATION FOR THE PROTECTION OF INFORMATION

***Maksimovskiy A.Yu.*[2]**

AbstractIn this paper, the properties of two classes of finite automata, which are generalizations of the feedback with carry shift register with transfer (memory) (FCSR), are investigated. These classes were constructed on the basis of the established isomorphism of the FCSR and the shift register over the ring of integers, as well as the exponential representation of the output sequence of the FCSR and the previously unknown properties of the output sequences of the FCSR. The necessary and sufficient conditions for the existence of diagnostic and setup experiments for the proposed generalizations of FCSR the estimation of the length of these experiments and the complexity of their implementation, the estimated number of operations in the corresponding rings. These parameters characterize the time and resource complexity of control procedures for the operation of devices, mathematical models of which are considered machines. It is shown that the efficiency of using the reverse operation to solve these problems depends significantly on the structure of the rings over which these automata are constructed. For one of the classes of generalized FCSR the method of finding prohibitions of output sequences is proposed, which allows to expand both the list of parameters of such devices to be monitored in the course of their operation, and their functionality in order to identify hidden channels of information leakage and organization of countering these threats to the security of information systems.

Keywords: *feedback with carry shift register, experiments with automata, prohibitions of automata, isomorphisms and automorphisms of automata, hidden channels of information leakage*

References

1. A.Klapper, M.Goresky. Feedback Shift Registers, 2-Adic Span, and Combiners with Memory. J.Cryptology, 1997, v.10, N 2, pp. 111-147.
2. A.Klapper, M.Goresky. Feedback Shift Registers, 2-Adic Shift Registers. Fast Software Encryption. // Lectures Notes in Computer Science. 1994. V.809, Springer Verlag, N. Y. , pp. 174-178.
3. Marsaglia G. Zaman A. A New Class of Random number Generators.// Ann. Appl. Prob., 1991, 1, pp 462-480.
4. Couture R., L'Ecuyer. On the Lattice Structure of Certain Linear Congruential Sequences Related to AWE/SWB Generatjr // Mathemftics for Computation., 1994, Vol. 62, N. 206, pp 799-808
5. A.Klapper, Jinzhong Xu. Algibraic Feedback Shift Registers. Theoretical computer Science, 1999, 226, pp. 61-92.
6. A.Klapper, Jinzhong Xu. Register Synthesis for Algibraic Feedback Shift Registers. Design, Codes and Cryptography, 2004, 31(3), pp. 227-250.
7. A.Klapper, M.Goresky. Algabraic Shift Register Sequences. Cf.mbridge University Press. 2012, 514 p.
8. Shreier Bryus Prikladnaya kriptografiya. Protokoly, algoritmy i teksty na yazyke C. – Vilyams, 2016. – 1024 p.
9. Pososhin V.A., Kuznetsov V.M., Gumirov A.I. Generatory psevdosluchainyh posledovatelnostei nemaksimolnoi dliny na registrah sdviga s vnutrennim summirovaniem po modulyu dva (chast 1) // Vestnik Chuvashskogo universiteta. 2017. № 1. pp. 263-272.
10. Chen W.-K. The VLSI Handbook, Second Edition. - CRC Press. - Chicago. - 2006. – 2320 p.
11. Grishkin A.S. Generatory psevdosluchainyh simvolov nemaksimolnoi dliny na registrah sdviga s vnutrennimi summatorami po modulyu dva pri ispolzovanii inversnyh vyhodov. // Dis. ... k.t.n., 05.13.05 – Elementy I ustroistva vychislitelnoi tehniki b system upravleniya, , Kazan, KGTU, 2006, 142 c.
12. Maksimovskiy A.Yu., Melnikov S.Yu. Spektralnye I kombinatornye svoistva redutsirovahhyh grafov de Breina // Voprosy Kiberbezopasnosti [Cybersecurity issues]. 2018. No 4, pp. 70-76. DOI: 10.21681/2311-3456-2018-4-70-76.
13. Liu M. Homomorphisms and automorphisms of 2-D de Bruijn-Good graphs // Discrete Mathematics, Vol.85, I.1, 1990, pp. 105-109.
14. Gill A. Vvedenie v teoriyu konichnyh avtomatov. M. Nauka, 1966, 272p.
15. Maksimovskiy A.Yu. O gruppovyh svoivvah podstnovok, opredelennyh na smezhnyh klassah konechnoi abelevoi grurry po ee podgruppam. Matematicheskie voprosy kriptografii, 2016, Vol.7, No 1, pp. 83-92.
16. Gill A. Lineinye posledovatelnostnye mashiny M. Nauka, 1974, 288p.
17. Lidl R., Nideerraiter G. Konechnye polya. V 2-h tomah; V. 2 – M. Mir. – 822p.
18. Bleihut R. Teoriya и praktika kodov, kontroliruyuschih oshibki M: Kniga po trebovaniyu, 2013. 566 p.
19. Kamlovskiy O.V., Kuzmin A.S. Otsenki chastot poyavleniya elementov v lineinyh rekurrentnyh posledovatelnostyah nad koltsami Galua // Fundament. i prikl. matem. . – 2000. –V. 6, vyp.4, – pp.1083–1094.
20. Sumarokov S.N. Zaprety dvoichnyh funktsiy I obratimost dlya odnogo klassa kodiruyucshih ustroistv Сумароков С. Н. // Obozrenie prikl. I prom. matem.. - 1994. - V.1 – Vyp. 1, pp. 33-55.
21. Babash A. V. Zaprety avtomatov i dvoichnyh funktsiy // Trudy po diskr. matem., 2006, V 9, pp.7–20
22. Babash A. V. Zaprety avtomatov // Matem. zametki, 2012, Vol 91, Vypusk 5, C. 667–673.
23. Parhomenko D.V. Gistogrammnaya funktsiya avtomata i ee prilozhiniya // Dis. ... K.f.-m.n. 01.01.09 – Diskretnaya matematika I matematicheskaya kibernetika, Moskva: MGU, 2015. – 86 p.
24. Grusho A.A., Grusho H.A., Timonina E.E. Vklyuchenie novyh zapretov v sluchainye posledovatelnjsti новых запретов в случайные последовательности // Inform. i ee primen., 2014. 8:4, pp. 46-52.

2 Alexander Yu. Maksimovskiy, Ph.D. (Math.), Associate Professor, Institute for Management Problems V.A. Trapeznikova RAS, Moscow, Russia. E-mail: almxmwxy@mail.ru.