Министерство образования и науки РФ
ФГАОУ ВПО «Казанский (Приволжский) федеральный университет»
Институт вычислительной математики и информационных технологий
Кафедра системного анализа и информационных технологий

Р.Х. Латыпов, Е.Л. Столов

Генерация криптографических ключей

Учебно-методическое пособие
Предназначено для студентов 4 курса Института
вычислительной математики и информационных технологий

Казань 2014

УДК 511, 519.6

Печатается по решению редакционно-издательского совета ФГАОУВПО
«КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»,
методической комиссии факультета вычислительной
математики и кибернетики, протокол № 4 от 11 декабря 2014 г.

Авторы-составитель —
докт. техн наук, проф. каф. САИТ КФУ Р.Х. Латыпов
докт. техн наук, проф. каф. САИТ КФУ Е.Л.Столов

Рецензент —
докт. физ.-мат. наук, проф. Ш.Т.Ишмухаметов

Р.Х. Латыпов, Е.Л.Столов
Генерация криптографических ключей: учебное пособие / Р.Х. Латыпов,
Е.Л.Столов.– Казань: Казан. ун. 2014.– 39 с.

Предназначено для студентов старших курсов факультета вычислительной математики и кибернетики.

Содержание

1 Введение

Генерация криптографического ключа является составной частью любой системы защиты информации. Иногда к этому ключу предъявляются дополнительные требования, например,представление в виде произведения двух простых чисел, однако, часто единственным требованием является случайность сгенерированной последовательности. На практике, вместо случайных чисел часто используют псевдослучайные числа. Способам создания генераторов псевдослучайных чисел посвящены многочисленные работы. В первой части данной главы кратко остановимся на методах порождения таких чисел и проблемах, связанных с возможностью восстановления последовательности по ее части. В основном речь пойдет об устройствах на основе сдвиговых регистрах с обратными связями. С математической точки зрения это теория линейный последовательностных машин (ЛПМ). Теория таких устройств нашла освещение в многочисленных статьях и монографиях, в связи с чем рассмотрение указанных устройств носит обзорный характер. Теория генераторов, использующих физические датчики, также разработана достаточно хорошо, но она гораздо меньше представлена в учебной литературе. Лишь недавно опубликована монография [?], где рассматриваются различные способы реализации таких датчиков. Однако, там основное внимание уделяется технической стороне вопроса. Теории физических датчиков посвящена большая часть данной главы. Во второй части рассматривается гибридный подход, когда используется физический датчик случайных чисел и преобразующая его ЛПМ. Такие датчики принято называть комбинированными генераторами псевдослучайных чисел (КГПСЧ) [?]. При этом не уточняется тип физического источника случайных величин.

В третьей части рассматривается конкретный тип источника случайных чисел, основанный на работе комбинационной схемы в режиме "дребезжания"(jittering). Четвертая часть посвящена возможности применения аппаратуры, работающей в трехзначной логике, для создания датчиков случайных чисел.

При работе с объектами линейной алгебры в данной главе приняты следующие обозначения. Вещественные или комплексные числа обозначаются строчными латинскими буквами, векторы обозначаются жирным латинским шрифтом либо буквами греческого алфавита. Например, вектор-строка, имеющий n компонентов, записывается в виде $\mathbf{a} = \langle a_1, \ldots, a_n \rangle$, либо как $\xi = \langle a_1, \ldots, a_n \rangle$ Матрицы обозначаются прописными латинскими буквами. Элемент матрицы A, стоящий в строке с номером i и столбце с номером j, обозначается символом $A[i|j]$. Строка с номером i и столбец с номером j обозначается символами $A[i|*]$ и $A[*|j]$ соответственно. Единичная матрица обозначается символом I, а диагональная матрица с элементами $d_1, \ldots, d_n$ обозначается как $diag(d_1, \ldots, d_n)$. Последовательности рассматриваются, как матрицы. Символ $A[p]$ означает элемент последовательности A с индексом p. Часть вычислений производится с вещественными и комплексными числами, а часть — в поле $GF(2)$ вычетов по модулю 2. Умножение во всех полях обозначается одинаково, но для сложения в поле $GF(2)$ будет применяться символ $\oplus$.

От читателя требуются знания в объеме стандартных курсов линейной алгебры, тео-

рии вероятностей и дискретной математики, преподаваемых на математических и инженерных факультетах. Все понятия, выходящие за пределы этих курсов, объясняются, и даются необходимые ссылки. Все необходимые вычисления в приводимых примерах осуществляются с помощью открытого математического пакета SciLab [?].

1.1 Матрицы с неотрицательными элементами

В процессе исследования свойств генераторов будет существенно использоваться теория матриц с неотрицательными элементами. Все необходимые сведения вместе с доказательствами можно найти в [?],[?] и [?]. Здесь будут приведены основные факты, относящиеся к этим объектам.

Определение 1 *Матрица A называется неотрицательной (положительной), если все элементы этой матрицы неотрицательные (положительные) числа. Эти условия записываются, как $A \geq 0$ и $A > 0$ соответственно.*

Определение 2 *Неотрицательная квадратная матрица A называется разложимой, если существует матрица перестановки P такая, что*

$$P^T \cdot A \cdot P = \begin{pmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{pmatrix},$$

в противном случае матрица называется неразложимой

Из определения следует, что если матрица A является разложимой, то тоже самое справедливо и для любой ее степени, и матрица $I + A$ также будет разложимой. С другой стороны, справедливо

Предложение 1 *Если матрица A порядка n является неразложимой матрицей, то*

$$(I + A)^{n-1} > 0 \tag{1}$$

Другими словами, условие (1) является необходимым и достаточным для неразложимости неотрицательной матрицы

Другой признак неразложимости дает

Предложение 2 *Неотрицательная матрица A будет неразложимой тогда и только тогда, когда для любой пары индексов i, j существует натуральное число q свое для каждой пары такое, что $A^q[i|j] > 0$*

Теорема 1 *Если A неразложимая матрица, то существует вещественное характеристическое число r этой матрицы такое, что имеет место неравенство $|c| \leq r$ для любого другого характеристического числа с этой матрицы, число r является простым корнем характеристического уравнения, и ему принадлежит собственный вектор α матрицы A с положительными элементами.*

Определение 3 *Матрица $A \geq 0$ называется стохастической, если*

$$(\forall i)\ \sum_k A[i|k] = 1$$

и дважды стохастической, если стохастическими являются матрицы A и A^T

Для неразложимой стохастической матрицы $r = 1$.

1.2 Генерация псевдослучайных чисел

При изложении данного параграфа будем следовать книге [**?**]. С математической точки зрения генераторы псевдослучайных чисел работают следующим образом. Имеется автономный конечный автомат $\Xi = (Y, Q, \delta, \lambda, q_0)$. Здесь Y – выходной алфавит, Q – конечное множество состояний, $\delta : Q \to Q$ – функция переходов автомата, $\lambda : Q \to Y$ – функция выхода, q_0 – начальное состояние. Перед началом работы Ξ устанавливается в начальное состояние. Время считается дискретным. Если в некоторый момент времени n автомат находится в состоянии q_n, то в этот момент времени на выходе автомата появляется сигнал $y_n = \lambda(q_n)$, а в момент времени $n+1$ автомат окажется в состоянии $q_{n+1} = \delta(q_n)$. Часто для описания автомата вместо функции δ используют диаграмму переходов. Это направленный граф, вершинами которого являются состояния автомата, а дуга из вершины q в вершину q' присутствует тогда и только тогда, когда $\delta(q) = q'$. Очевидно, что из каждой вершины выходит только одна дуга, но возможно, что в некоторую вершину входят несколько дуг. Вся диаграмма переходов распадается на несколько связных компонент. Если в каждую вершины компоненты входит только одна дуга, то такая компонента называется циклической, или кольцевой.
В силу конечности числа состояний автомата, какое-то состояние должно повториться — для некоторых целых n, p будет выполнено равенство $q_n = q_{n+p}$. Это означает, что для любого натурального числа k выполнено равенство $y_{n+k} = y_{n+p+k}$. В дальнейшем последовательность на выходе становится периодической с периодом p. Указанное свойство является принципиальным недостатком любого генератора псевдослучайных чисел, поэтому при проектировании устройства стараются сделать параметр p как можно большим. Достоинством данного метода является простота его реализации на компьютере и возможность повторить сгенерированную последовательность столько раз, сколько надо. Все математические пакеты содержат подобного рода генераторы, реализующие один из алгоритмов. Как правило, генератор должен создавать равномерное распределение на интервале [0,1], поскольку из такого генератора можно получить теоретически любое другое распределение. Для получения равномерности достаточно потребовать выполнения следующего условия: диаграмма переходов является кольцом большой длины. Действительно, если $|Q| = r$, то перенумеруем произвольным образом все состояния числами от 1 до r и положим $\lambda(q_i) = i/r, \quad i = 1, \ldots r$. В этом случае в результате прохода по кольцу получим на выходе каждое из чисел i/r ровно один раз. Однако, одной равномерности не

достаточно, требуется чтобы числа на выходе были "независимыми". Формально ни о какой независимости не может быть и речи, поскольку полученная последовательность является детерминированной. В этой связи под независимостью понимают прохождение полученной последовательности через несколько статистических тестов. Рассмотрим два наиболее распространенных и простых в применении теста.

1.3 Автокорреляционная функция

Напомним известный из теории вероятности факт. Имеются две независимые случайные величины ξ и η с нулевым средним. В этом случае $E(\xi\eta) = 0$. Пусть имеется генератор псевдослучайных величин $x_n = f(n)$. Полученные числа рассматривают как реализацию некоторого стационарного случайного процесса с нулевым средним. Функция $R(p) = E(x_n x_{n+p})$ называется автокорреляционной функцией процесса. Если случайные величины x_n и x_{n+p} независимы, то $R(p) = 0, p > 0$. При изучении свойств конкретного устройства либо подсчитывают теоретическое значение функции

$$R_r(p) = \frac{1}{r}\sum_{k=1}^{r} x_k x_{k+p} \tag{2}$$

(напомним, что в (2) последовательность x_n является периодической с периодом r) либо выбирают отрезок длины m сгенерированной последовательности и подсчитывают

$$R_m(p) = \frac{1}{m}\sum_{k=1}^{m} x_k x_{k+p}, \tag{3}$$

дополняя, если необходимо, полученную последовательность нулями. Если условие $R_m(p) \to 0, \quad m \to \infty$ не выполнено, то тест на независимость не проходит, хотя близость этой величины к нулю не обеспечивает независимость. На практике проверяют отсутствие отдельных пиков в графике функции $R_m(p)$. Наличие пика в точке p_0 означает зависимость между значениями с шагом p_0. Отметим, что вычисления в (3) производятся с помощью быстрого преобразования Фурье (FFT) (например, см. [?]). С этой целью берется вектор длины $2m$

$$\langle x_1, \ldots, x_m, 0, \ldots, 0\rangle.$$

вычисляется преобразование Фурье $\mathbf{F}$ от этого вектора, которое само является вектором длины $2m$, поэлементно перемножаются компоненты векторов $\mathbf{F}$ и $\bar{\mathbf{F}}$ – состоящего из сопряженных чисел – и берется обратное преобразование Фурье от этого вектора. Последовательность, образованную из компонентов вектора обозначим через G. В результате

$$R_m(p) = \frac{1}{m-p}G[p], \quad p = 0, \ldots, m/2 \tag{4}$$

Появление коэффициента в (4) обусловлено тем, что из-за наличия нулей реальное количество слагаемых в (4) уменьшается с ростом p. Применим этот метод для

проверки качества стандартного датчика псевдослучайных чисел, реализованного в пакете SciLab. В консоли введем следующий скрипт (номера операторов вводить не надо)

```
N=200; //1
x1=rand(1,N,'normal');//2
 x2=[x1,zeros(1,N)];//3
fx2=fft(x2);//4
cfx2=conj(fx2);//5
prd=fx2.*cfx2;//6
crr=real(ifft(prd));//7
K=N:-1:1; //8
auto=crr(1:N)./K;//9
plot(auto)//10
```

Поясним смысл операторов.

1. выбор длины исследуемой последовательности
2. генерация N псевдослучайных чисел, имеющих нормальное распределение с нулевым средним и единичной дисперсией
3. добавление N нулей
4. вычисление преобразования Фурье
5. нахождение сопряженного массива чисел
6. поэлементное умножение
7. вычисление обратного преобразования Фурье и выделение вещественной части; формально, должно получиться вещественное число, но возможно появление комплексной части из-за ошибок округления
8. создание массива чисел от N до 1
9. поэлементное деление двух массивов
10. график получившегося массива представлен на Рис.1

Обратим внимание на на большую разницу в значениях $R(0)$ и $R(p)\, p \neq 0$. Исключение составляют числа в конце массива. Это связано с тем, что указанные значения получаются усреднением по малому количеству слагаемых. Оценка качества в данном случае осуществляется визуально. Следующий способ позволяет дать численную оценку качества генератора.

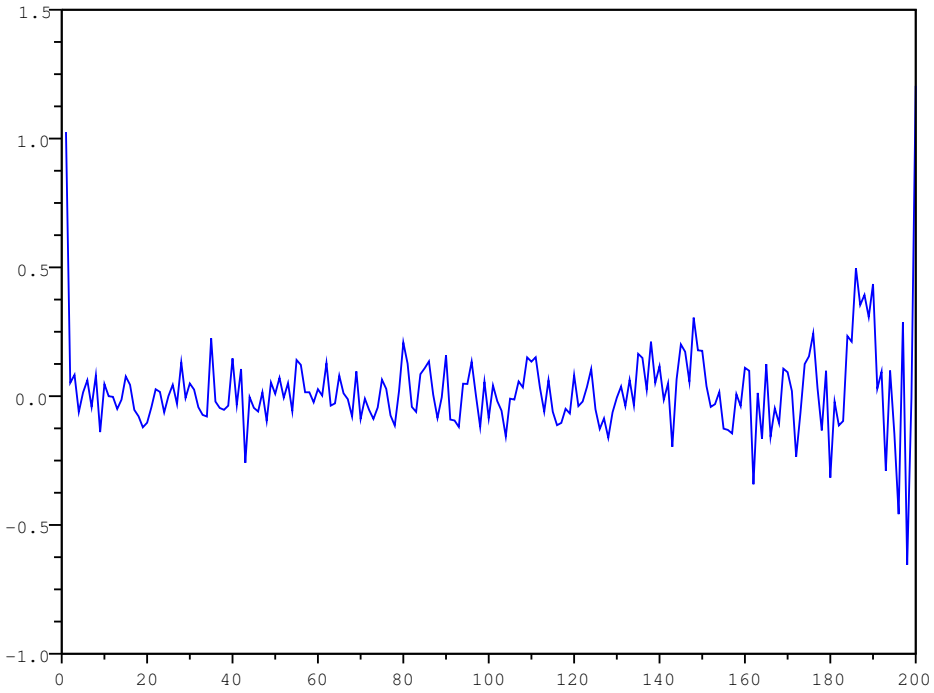

Рис. 1: Автокорреляционная функция

1.4 Критерий χ^2

Значительная часть критериев независимости случайных величин основана на распределении χ^2_n. Напомним, что это распределение имеет величина

$$\xi_n = \sum_{k=1}^{n} \eta_k^2,$$

где η_k независимые случайные величины с нормальным распределением нулевым средним и единичной дисперсией. Различные критерии основаны на следующем факте [?]. Пусть имеются n независимых случайных величин μ_k, имеющих одно и то же распределение. Разобьем область значений случайных величин на q частей: $S_1, S_2, \ldots, S_q$. Обозначим через p_i вероятность $p_i = P(\mu \in S_i)$, а через n_i количество величин $\mu_k \in S_i$, действительно попавших в это множество в результате эксперимента. Тогда значение

$$v = \sum_{i=1}^{q} \frac{(n_i - np_i)^2}{np_i} \tag{5}$$

имеет распределение близкое к χ^2_{q-1} для больших n. Выбирается уровень значимости, например, 5 процентов. По таблицам находят значение z, для которого выполнено равенство $P(\xi_{q-1} > z) = 0.05$. Если окажется, что выполнено неравенство $v > z$, гипотезу о равномерности распределения величин μ_k отвергают, в противном случае ее принимают.

Покажем, как общая схема применяется для проверки качества генератора. Выбирается начальное состояние генератора и длина последовательности. Последняя должна быть значительно меньше общей длины кольцевой компоненты, которой принадлежит начальное состояние. Предположим, что все порожденные значения x_k находятся в интервале [0,1]. В этом случае этот интервал разбивается произвольным образом на q частей $S_i, i = 1, \ldots, q$, вычисляется значение согласно (5) и проверяется справедливость гипотезы. Эксперимент повторяется многократно при различных начальных состояниях.

Более тонкий способ проверки выглядит следующим образом [**?**]. Выбирается натуральное число w и строятся векторы вида

$$\mathbf{b_1} = \langle x_1, \ldots, x_w \rangle, \mathbf{b_2} = \langle x_{w+1}, \ldots, x_{2w} \rangle, \ldots$$

w-мерный куб разбивается на q частей $S_i, i = 1, \ldots, q$ и снова подсчитывается значение (5) для величин $\mathbf{b_k}$, после чего справедливость гипотезы о равномерности оценивается прежним способом. Следует отметить, что создание генератора, проходящего указанный тест для больших w является серьезной проблемой.

В качестве примера осуществим проверку того же датчика, но используя изложенный критерий.

В SciLab в консоли выпишем следующий скрипт

```
N=200;//1
x=rand(N,4);//2
buff=zeros(1,16);//3
pows=[1,2,4,8];//4
for k=1:N //5
    flags=zeros(1,4); //6
    str=x(k,:);//7
    for i=1:4//8
        if(str(i)>0.5),flags(i)=1;end//9
    end//10
    numb=1;//11
    for i=1:4  //12
        numb=numb+flags(i)*pows(i);//13
    end//14
    buff(numb)=buff(numb)+1;//15
end//16
```

Операторы 1-2 порождают матрицу x размера $N \times 4$, составленную из псевдослучайных чисел с равномерным распределением на [0,1]. Четырехмерный единичный куб

разделим на 16 равных частей. Вектор длины 4 $\eta = \langle a_1, a_2, a_3, a_4 \rangle$ попадает в ту или иную часть, в зависимости от того, справедливо ли неравенство $a_i < 0.5$, $i = 1, 2, 3, 4$. Оператор 3 создает массив $buff$, в котором элемент $buff(j)$, $j = 1, \ldots, 16$ показывает, сколько векторов из выборки попало в часть с номером j. Оператор 6 создает массив, в котором будет записан в двоичной форме номер области, в которую попал очередной вектор. Оператор 7 выделяет очередную строку, а операторы 8-10 формируют двоичный номер. Операторы 11-14 переводят двоичный номер в обычное число. Единица добавляется в номер, поскольку все индексы начинаются с 1.
После того, как будет сформирован $buff$, надо применить критерий χ^2 для проверки гипотезы о равномерности распределения векторов по областям. В данном случае попадание в каждую область равно $p_i = 1/16$. Чтобы применить формулу (5), надо выполнить следующий скрипт

```
buff1=buff-N/16;//1
v=sum(buff1.*buff1)/(N/16); //2
```

Оператор 1 вычитает из всех элементов $buff$ одно и то же число, а оператор 2 завершает подсчет по формуле (5).
Полученное число v надо сравнить с порогом, определенным уровнем значимости. Для этого выбираем этот уровень, например 0.05, и подсчитываем порог с помощью встроенной функции SciLab. Вводим

```
val=cdfchi("X",15,0.95,0.05)
```

Здесь 15=16-1 — число степеней свободы, два оставшиеся числа определяют уровень значимости (их сумма всегда 1, но порядок следования аргументов существенен). Если окажется, что $v > val$, гипотеза отвергается. Конечный результат зависит от начального состояния генератора псевдослучайных чисел. В проведенном эксперименте получилось значение $v = 20$, в то время как $val = 24.99$. Это означает, что гипотеза о равномерности попадания векторов в каждую область надо принять. Интересно провести проверку для векторов, длина которых порядка 20-30, но для этого нужен достаточно мощный компьютер.

1.5 Способы построения генераторов

Рассмотрим два наиболее распространенных способа построения генераторов псевдослучайных чисел. Первый из них ориентирован на применение компьютера, а второй — на аппаратную реализацию.

1.5.1 Мультипликативный датчик

Мультипликативный датчик выглядит следующим образом [?]. Выбираются натуральные числа q, a, n, x_0. Множество состояний автомата состоит из целых чисел $0, 1, \ldots, q-1$. Состояния меняются согласно формуле

$$x_k = (a * x_{k-1} + n) \pmod q \quad k = 1, 2, \ldots$$

Функция выходов $\lambda(x) = x/(q-1)$. В результате сгенерированные числа принадлежат интервалу [0,1]. Рекомендации по выбору параметров q, a, n представлены в [?]. Следует отметить, что эти рекомендации учитывают как статистические свойства порожденных последовательностей, так и оптимизацию скорости вычисления с учетом архитектуры процессора. Читателю предлагается проверить какой-либо из рекомендуемых датчиков по схеме, представленной выше.

1.5.2 Датчик на основе линейной последовательнстной машины (ЛПМ)

Обозначим через $GF(2)$ поле вычетов по модулю 2. Выбираются натуральные числа n, m, k. Согласно [?], ЛПМ определяется матрицами A, B, C, с элементами из поля $GF(2)$, где A $n \times n$ матрица, матрицы B, C имеют размерности $n \times m$ и $k \times n$ соответственно. Состояния ЛПМ суть векторы длины n $\mathbf{q} = \langle q_1, \ldots, q_n \rangle^T$, где $q_i \in GF(2)$, а входной и выходной алфавиты состоят из аналогичных векторов длины m и k соответственно. Состояние меняется согласно формуле

$$\mathbf{q_k} = A\mathbf{q_{k-1}} \oplus B\mathbf{x_k}, \tag{6}$$

а выходной сигнал вычисляется согласно

$$\mathbf{y_k} = C\mathbf{q_k} \tag{7}$$

В формулах (6),(7) все матричные операции осуществляются в поле $GF(2)$. Если требуется, чтобы на выходе генератора было число из интервала [0,1], выходной двоичный вектор $\mathbf{y}$ интерпретируют как двоичную запись числа $0.y_1, \ldots, y_k$. В случае автономной ЛПМ матрица $B = \Theta$, а состояние меняется согласно

$$\mathbf{q_k} = A\mathbf{q_{k-1}} \tag{8}$$

Очевидно, что если начальное состояние генератора (8) выбрано нулевым, то генератор не выйдет из этого состояния. Оказывается, что можно выбрать матрицу A таким образом, чтобы диаграмма переходов состояла лишь из двух компонент: нулевого вектора и кольцевой диаграммы переходов, куда входят все остальные состояния. В этом случае говорят, что генератор имеет максимальный период.
В [?] указано как осуществить выбор матрицы A, чтобы генератор имел максимальный период. Достоинством указанной схемы является ее простая аппаратная реализация. Действительно, предположим, что матрица

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & 0 & 1 \\ a_n & a_{n-1} & a_{n-2} & \ldots & a_1 \end{pmatrix} \tag{9}$$

Если $\mathbf{q_{k-1}} = \langle q_1, q_2, \ldots, q_n \rangle^T$, то согласно (8) $\mathbf{q_k} = \langle q_2, q_3, \ldots, f \rangle^T$, где

$$f = \oplus \sum_{i=1}^{n} a_i q_{n+1-i} \tag{10}$$

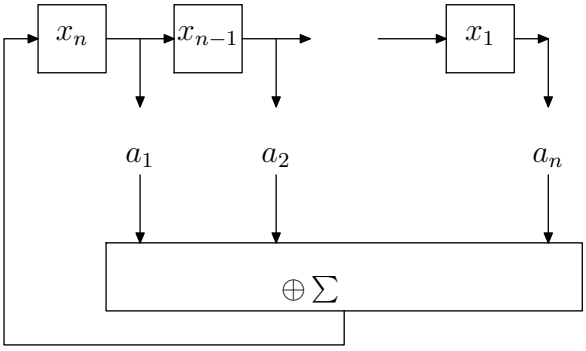

Рис. 2: Пример реализации датчика на основе регистра сдвига

Изменения состояний ЛПМ указанного вид иногда удобнее рассматривать как последовательность, порождаемую рекуррентным соотношением. Имеются элементы $q_0, q_1, \ldots, q_{n-1} \in GF(2)$. Следующий элемент последовательности получается согласно формуле

$$q_k = \oplus \sum_{i=1}^{n} a_i q_{k-i},\ k = n, n+1, \ldots \tag{11}$$

Рассмотрим схему, представленную на Рис.2. Она состоит из n элементов памяти, организованных в виде регистра сдвига, умножителей на коэффициенты и комбинационной схемы $\oplus\sum$, суммирующей поступающие сигналы. Состоянием автомата является набор битов, находящихся в элементах памяти. В следующий момент времени происходит сдвиг содержимого регистров вправо, а элемент памяти x_n вычисляется согласно (10). При подходящем выборе матрицы A выполнены тесты на равномерность и на независимость в терминах автокорреляционной функции [?]. Различные реализации автоматов указанных типов и свойства порождаемых последовательностей представлены в [?] .

С математической точки зрения, не имеет значения, какая матрица будет обеспечивать максимальный период генератора. Однако, с точки зрения реализации полезно выбрать матрицу A таким образом, чтобы число ненулевых элементов в ней было минимальным. Действительно, каждый ненулевой элемент в этой матрице означает физическое соединение блоков. Нижнюю строку матрицы (9) принято задавать в виде многочлена

$$Pol(x) = x^n \oplus \sum_{k=1}^{n} x^n$$

Эти многочлены называются многочленами максимального показателя. В [?] приведены многочлены для некоторых n, для которых многочлен $Pol(x)$ имеет только 3 ненулевых коэффициента. Например,

$$1 \oplus x \oplus x^3,\ 1 \oplus x^2 \oplus x^5,\ 1 \oplus x^5 \oplus x^{23}.\ 1 \oplus x^{11} \oplus x^{36}$$

Читателю предлагается оценить качество генератора, используя приведенную выше технику.

1.6 Применение генераторов псевдослучайных чисел для порождения криптографических ключей

Как было указано выше, последовательность порождаемая генератором псевдослучайных чисел, полностью определяется начальным состоянием. Для обеспечения "случайности"всей последовательности случайным образом порождают начальное состояние. В частности, в качестве начального состояния часто берут младшие разряды таймера. Однако, для целей криптографии важно обеспечить невозможность восстановления всей последовательности по ее части. Во всех рассмотренных выше случаях, вся последовательность легко восстанавливается по одному состоянию. Дело не спасает, если в качестве выхода генератора брать не все состояние, а только его часть, например, только один бит или линейную комбинацию битов над полем $GF(2)$. Пусть выход генератора (8) в момент времени k определяется формулой

$$y[k] = C\mathbf{g_k},$$

где $\mathbf{q_k} = \langle q_1, q_2, \ldots, q_n\rangle^T$-состояние генератора в момент времени k, а $C = (c_1, c_2, \ldots, c_n)$, $C \neq \Theta$. Заметим, что при анализе криптостойкости всегда считается известной структура генератора. В данном случае это означает, что известны матрицы A и C. Положим

$$\bar{A} = \begin{pmatrix} C \\ CA \\ CA^2 \\ \ldots \\ CA^{n-1} \end{pmatrix}$$

Предположим, что имеет место равенство

$$\mathrm{rank}(\bar{A}) = n \tag{12}$$

Это условие называется условием наблюдаемости ЛПМ [?]. Если $\mathbf{q_0}$ начальное состояние, то столбец $\mathbf{y}$, составленный из первых n битов имеет вид

$$\bar{A}\mathbf{q_0} = \mathbf{y}$$

В силу невырожденности матрицы $\bar{A}$ начальное состояние восстанавливается по первым n последовательным битам.

От указанного недостатка пытаются избавиться включением какой-либо нелинейности в структуру генератора. Простейшая схема, обеспечивающая цикличность, предложена Голомбом [?]. В терминах рекуррентных последовательностей (11) формула имеет вид

$$q_k = q_{k-n+1} \oplus f(q_{k-1}, \ldots, q_{k-n+2}),$$

где $f()$ произвольная булевская функция. Данная формула гарантирует цикличность каждой компоненты в диаграмме переходов. В этом случае не очевиден алгоритм восстановления начального состояния по выходной последовательности. В то же время возникают проблемы с доказательством статистических свойств выходной последовательности. Некоторые примеры исследования подобных регистров представлены в [?]. Обобщение формул Голомба, также обеспечивающих цикличность всех компонент, представлено в [?].

1.7 Комбинированные генераторы псевдослучайных чисел КГПСЧ

Несмотря на простоту генерации псевдослучайных криптографических ключей, в тех случаях, когда требуется высокая степень защиты, используют случайные ключи, порожденные некоторым физическим процессом. Как отмечалось выше, требуется, чтобы отдельные символы имели равномерное распределение и были независимыми. В данной главе рассмотрим ситуацию, когда некоторый физический датчик выдает независимые сигналы, но вероятность каждого из них колеблется в некоторых пределах.

1.8 Постановка задачи

Пусть имеется конечный автомат $\Xi(X, Y, Q, \delta, \lambda, q_0)$, где X, Y входной и выходной алфавиты соответственно, функция переходов $\delta : X \times Q \to Q$, функция выходов $\lambda : Q \to Y$, начальное состояние q_0. Имеется случайный процесс $\xi(t)$, принимающий значения из множества X, случайные величины $\xi(t_1), \xi(t_2)$ являются независимыми для $t_1 \neq t_2$, но имеют, вообще говоря, разные распределения. Предполагается, что вероятность $p_x(t) = P(\xi(t) = x \in X)$ заключена в некотором интервале

$$0 < a_x \leq p_x \leq b_x < 1, \tag{13}$$

не зависящем от t. Случайные сигналы поступают на вход автомата Ξ, в результате последовательность состояний автомата $q(t)$ образует неоднородную цепь Маркова [?]. Идея выравнивания вероятностей с помощью автомата заключается в следующем [?]: выбирается натуральное m, и сигналы с выхода автомата снимаются с этим шагом. Полученные сигналы становятся случайными величинами. Оказалось, что при некоторых естественных предположениях вероятность появления любого символа алфавита Y на выходе становится одной и той же, а сами случайные величины, будут независимыми. Последние утверждения выполняются лишь с некоторой точностью. Строгое определение этого понятия будет дано ниже.

1.9 Случай линейной последовательностной машины

Рассмотрим ситуацию, когда в качестве автомата выбрана ЛПМ. Случай, когда в качестве ЛПМ был выбран регистр сдвига с обратными связями, подробно рассмот-

рен в [**?**]. Имеется ЛПМ, состояния которой есть векторы длины n над $GF(2)$. Для простоты изложения предположим, что входной алфавит Y состоит лишь из двух символов [0,1] и кодируется вектором длины 1. В силу этого матрица B в (6) будет столбцом длины n.. Пусть в момент времени t_s ЛПМ находится в состоянии $\mathbf{q_s}$. В этот момент с некоторой вероятностью p_0 на вход ЛПМ поступит сигнал 0 и с вероятностью p_1 поступит сигнал 1. Это означает, что с вероятностью p_0 $\mathbf{q_{s+1}} = A\mathbf{q_s}$ и с вероятностью p_1 $\mathbf{q_{s+1}} = A\mathbf{q_s} \oplus B$. С помощью этих соотношений строится матрица переходов $T(t_s)$ цепи Маркова . Это матрица размера $2^n \times 2^n$. Каждому состоянию ЛПМ отвечает одна строка и один столбец этой матрицы. Обычно состоянию $\langle q_1, \ldots, q_n \rangle^T$ ставится в соответственно номер строки или столбца, двоичный номер которых есть число $q_1 q_2 \ldots q_n$. Отметим, что номера строк и столбцов начинаются с 0. Обозначим через k, l, m номера строк, отвечающие состояниям $\mathbf{q_s}$, $A\mathbf{q_s}$, $A\mathbf{q_s} \oplus B$ соответственно. Матрица T имеет следующий содержательный смысл — из состояния с номером k ЛПМ перейдет в состояние с номером l с вероятностью p_0 и в состояние с номером m с вероятностью p_1, поэтому $T(t_s)[k|l] = p_0$, $T(t_s)[k|m] = p_1$. Чтобы сделать рассуждения более понятными, рассмотрим пример. Пусть $n = 3$,

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Согласно определению

$$T = \begin{pmatrix} p_0 & p_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & p_0 & p_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p_1 & p_0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_1 & p_0 \\ p_1 & p_0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & p_1 & p_0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p_0 & p_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_0 & p_1 \end{pmatrix}$$

Поясним вид строки с номером 1 матрицы T(напомним, что нумерация начинается с 0). Эта строка соответствует состоянию $\mathbf{q_1} = \langle 0, 0, 1 \rangle^T$. Находим $A\mathbf{q_1} = \langle 0, 1, 0 \rangle^T = \mathbf{q_2}$, и $A\mathbf{q_1} \oplus B = \mathbf{q_3}$. Это объясняет появление чисел p_0 и p_1 в столбцах с номерами 2 и 3. Как и следовало ожидать, сумма элементов в каждой строке матрицы T равна 1, то есть матрица является стохастической. Это имеет место для любой матрицы переходов цепи Маркова. Однако, в данном случае и сумма элементов в каждом столбце матрицы T также равна 1, то есть матрица является дважды стохастической. Последнее свойство справедливо для любой ЛПМ с невырожденной матрицей A. Действительно, в рассматриваемом случае выберем произвольное состояние $\bar{\mathbf{q}}$. Тогда для любого входного сигнала $\mathbf{x}$, равного значению случайного процесса $\xi(t)$, всегда существует решение $\mathbf{q}$ уравнения

$$A\mathbf{q} \oplus B\mathbf{x} = \bar{\mathbf{q}}$$

Это означает, что сумма элементов в столбце, отвечающем состоянию $\bar{\mathbf{q}}$, равна сумме вероятностей значений случайной величины $\xi(t)$, то есть равна 1.
Пусть известна реализация процесса ξ длины n, то есть известны случайные величины $\xi(0), \xi(1), \ldots, \xi(n-1)$. В результате ЛПМ перейдет из состояния $\mathbf{q_0}$ в состояние

$$\mathbf{q_n} = A^n \mathbf{q_0} \oplus A^{n-1} B\xi(0) \oplus A^{n-2} B\xi(1) \oplus \cdots \oplus B\xi(n-1) \tag{14}$$

Введем дополнительное ограничение на матрицы A и B. Предположим, что выполнено равенство

$$rank(A^{n-1}B, A^{n-2}B, \ldots, B) = n \tag{15}$$

Это свойство называют управляемостью системы [**?**]. Данное условие равносильно следующему – векторы вида

$$A^{n-1}B, A^{n-2}B, \ldots, B$$

составляют базу в пространстве столбцов длины n. Отсюда и из формулы (14) следует, что вектор $\mathbf{q_n}$ с положительной вероятностью может совпадать с любым столбцом длины n. С другой стороны, из определения цепи Маркова вытекает, что матрица

$$F_n = T(0)T(1)\cdots T(n-1)$$

дает распределение состояний автомата через n шагов. Строка $\langle 0, \ldots 0, 1, 0 \ldots 0 \rangle F_n$, где 1 стоит в позиции с номером k, состоит из распределения вероятностей состояний через n шагов, если первоначально систем находилась в состоянии с номером k. Как было указано выше, при сделанных предположениях ЛПМ может перейти за n шагов из любого состояния в любое состояние с положительной вероятностью. Другими словами, все элементы матрицы F_n положительны. Легко проверяется, что произведение двух дважды стохастических матриц есть снова дважды стохастическая матрица. Теперь из положительности элементов матрицы F_n вытекает, что

$$F_n^m \to T_\infty,\ m \to \infty, \tag{16}$$

где T_∞ – матрица ранга 1 [**?**]. Поскольку это дважды стохастическая матрица, все ее элементы равны $1/2^n$. Выберем m настолько большим, чтобы разность между элементами матриц T_∞ и F_n^m была меньше заданного числа Δ. Как было указано выше, матрицы $T(k)$ могут меняться вместе с k, поэтому величина m также будет варьироваться вместе с реализацией. Однако, в силу (13) можно получить оценку, не зависящую от реализации [**?**]. Положим $s = nm$. Если съем сигнала с выхода ЛПМ производится с шагом s, то можно утверждать, что с указанной точностью вероятность попадания ЛПМ в любое состояние будет одной и той же и не будет зависеть от предыдущего состояния, с которого снимался сигнал.

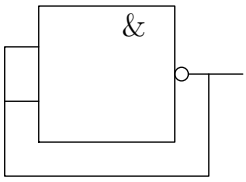

Рис. 3: Пример генератора на основе инвертора

1.10 Марковская модель генератора случайных чисел

1.10.1 Модель физического генератора случайных чисел

До сих пор физический источник случайных чисел оставался в стороне. В данном пункте будет описан один из таких источников, основанный на работе комбинационной схемы в нештатном режиме. Вероятно впервые, идея создания таких генераторов была предложена в [?] для комбинационных схем специального вида — линейных схем. Оказалось, что теория таких генераторов справедлива для схем весьма общего вида [?]. Эта теория представлена в данном пункте. Особенность теории генераторов на основе линейных схем будет изложена в следующем пункте.
Рассмотрим простейшую схему, изображенную на Рис.3. Она содержит инвертор на основе элемента И-НЕ, выход которого подключен к входу. С точки зрения обычной логики выход устройства не определен. Если же речь идет о физическом устройстве, то тут ситуация иная. Если на вход инвертора поступает единичный сигнал, то этот сигнал преобразуется в нулевой сигнал на выходе, но это преобразование происходит не мгновенно, а с некоторой задержкой. Аналогичный эффект имеет место, если на входы схемы подан нулевой сигнал. Это явление получило название "дребезжание". Предлагается математическая модель этого явления, которая заключается в том, что время t изменения выходного сигнала после изменения входного сигнала подчиняется экспоненциальному закону, то есть $P(t < t_0) = 1 - exp(-at_0)$, где a – параметр распределения. Это распределение обладает следующим замечательным свойством: $P(t < t_1 | t > t_0) = 1 - exp(-a(t_1 - t_0))$.
Содержательно последнее равенство означает следующее: если событие не произошло до момента времени t_0, то после этого момента время ожидания события подчиняется тому же самому закону. Это свойство марковости процесса, поскольку дальнейшее его поведения после момента времени t_0 зависит только от состояния процесса в этот момент времени и не зависит от предыдущей истории. На этом свойстве основаны уравнения Эрланга, с помощью которых в дальнейшем будет описано поведение генератора.

1.10.2 Уравнения Эрланга для описания поведения "дребезжащей"схемы

Рассмотрим схему, изображенную на Рис.4. Имеется комбинационная схема с n выходами и m входами, причем выходы произвольным образом соединены с входами

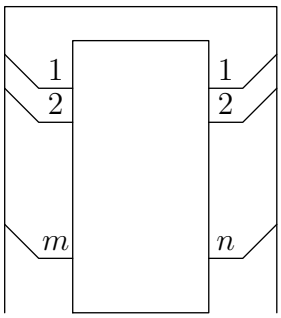

Рис. 4: Произвольная комбинационная схема в нештатном режиме

этой схемы (допускается, что на некоторые входы подан постоянный сигнал, а на несколько входов подан сигнал с одного выхода). В результате возможно, что схема перейдет в некоторое стабильное состояние (например, известная схема RS триггера), но возможно, что схема окажется в режим генерации. Будем рассматривать только второй случай. Сделаем следующие предположения [?]:

1. Время изменения сигнала на каждом выходе в результате изменения сигнала на входе, если это определяется логикой схемы, подчиняется экспоненциальному закону с одним и тем же параметром для всех выходов

2. В любой момент времени может измениться только один выход

3. Изменения сигналов на выходах являются независимыми событиями

Сделанные предположения о функционировании схемы позволяют описать динамику работы генератора с помощью дифференциальных уравнений, аналогичных уравнениям Эрланга в теории массового обслуживания (см., например, [?]). Составление этих уравнения проиллюстрируем на примере схемы, изображенной на Рис. 4, когда $m = n = 3$. Назовем состоянием $\mathbf{S(t)}$ генератора в момент времени t вектор $< y_1, y_2, y_3 >$, составленный из выходов трех элементов. На выходе с номером i реализуется булевская функция $f_i(y_1, y_2, y_3)$. Состояние генератора в следующий момент времени может измениться в результате изменения одного из выходов. Все возможные двоичные векторы-состояния перенумеруем, используя естественную двоичную нумерацию. Обозначим через $P_n(t)$ вероятность того, что в момент времени t генератор находится в состоянии с номером n. Рассмотрим некоторое состояние $< y_1, y_2, y_3 >$. Согласно сделанным предположениям, из данного состояния возможен переход в состояния $< f_1(y_1, y_2, y_3), y_2, y_3 >$, $< y_1, f_2(y_1, y_2, y_3), y_3 >$, и $< y_1, y_2, f_3(y_1, y_2, y_3) >$. Составим матрицу A переходов генератора. Как обычно, элемент этой матрицы, стоящий в строке с номером i и столбце с номером j, обозначим через $A[i|j]$. По определению этот элемент равен количеству переходов из состояния с номером i в состояние с номером j в результате изменения сигналов на выходах. При составлении этой матрицы учитываются также "виртуальные переходы". Под

виртуальным переходом мы понимаем ситуацию, когда при вычислении текущего значения булевской функции на выходе значение функции не меняется. Например, если $y_1 = f_1(y_1, y_2, y_3)$, то считается, что в результате такого виртуального перехода состояние генератора не изменилось. Виртуальным переходам отвечают диагональные элементы матрицы A. В силу сделанного замечания, сумма элементов в каждой строке матрицы A равна числу выходов схемы, поскольку учитываются как обычные переходы, так и виртуальные переходы.
В рассматриваемом случае схема имеет 3 выхода, и генератор может находиться в одном из 8 состояний. Вероятность того, что в момент времени $t+\Delta t$ генератор будет в состоянии с номером n величина $P_n(t+\Delta t)$ складывается из из вероятности того, что в момент времени t система находилась в том же состоянии, и после этого не сработал ни один выход, и из вероятностей нахождения в момент времени t в другом состоянии и срабатывании подходящего выхода. Учтем предположение об экспоненциальном распределении времени всех срабатываний. Отбрасывая величины порядка больше первого по Δt, получим, что вероятность не срабатывания всех выходов равна $1 - 3a\Delta t$, а вероятность срабатывания одного выхода равна $a\Delta t$. Имеем

$$P_n(t + \Delta t) = P_n(t)(1 - 3a\Delta t) + \sum_{k=0}^{7} a\Delta t A[k|n] P_k(t)$$

Деля на Δt и переходя к пределу при $\Delta t \to 0$, получим

$$\frac{dP_n(t)}{dt} = -3aP_n(t) + a\sum_{k=0}^{7} A[k|n] P_k(t), \quad n = 0, ..., 7$$

В общем случае, когда генератор имеет m выходов и $r = 2^m$ состояний, уравнение принимает вид

$$\frac{dP_n(t)}{dt} = -maP_n(t) + a\sum_{k=0}^{r-1} A[k|n] P_k(t), \quad n = 0, ..., r-1 \tag{17}$$

Заметим, что в (17) все виртуальные срабатывания исключаются. Если, например, при $m = 3$ имеются два виртуальных срабатывания в состоянии с номером n, то вероятность не срабатывания будет равна $1 - a\Delta t$. С учетом виртуальных срабатываний вероятность не срабатывания равна $1 - 3a\Delta t$, а $A[n|n] = 2$, и в результате, получается то же самое уравнение (17).

1.11 Финальный вектор марковского процесса

Обозначим через $\mathbf{P}(t) = \langle P_0(t), \ldots, P_{r-1}(t)\rangle$. Уравнение (17) в матричной форме имеет вид

$$\frac{d\mathbf{P}(t)}{dt} = a\mathbf{P}(t)(A - mI),$$

а его решение равно [?]

$$\mathbf{P}(t) = \mathbf{P}(0)e^{a(A-mI)t} \tag{18}$$

По построению

$$\sum_{i=0}^{N-1} A[k|i] = m, \quad k = 0, \ldots, r-1$$

и все элементы этой матрицы неотрицательны. Отсюда следует, что A/m – стохастическая матрица, m будет характеристическим числом матрицы A. Как было указано выше, все остальные характеристические числа b_i матрицы A удовлетворяют неравенствам

$$|b_i| \leq m, \quad i = 1, \ldots, r$$

В дальнейшем будем предполагать, что $b_1 = m$. Потребуем теперь, чтобы матрица A была неразложимой. Как следует из Теоремы 1, в этом случае число m будет простым корнем, поэтому справедливы неравенства

$$\mathrm{Re}(b_i) < m, \quad i = 2, \ldots, r, \tag{19}$$

а числу m отвечает собственный вектор-строка $\mathbf{Q} =< q_1, \ldots, q_N >$ с положительными элементами: $m\mathbf{Q} = \mathbf{Q}A$. Без ограничения общности можем предполагать, что вектор $\mathbf{Q}$ нормирован условием $\sum_k q_k = 1$. В матрице $A - mI$ одно характеристическое число равно нулю, а остальные характеристические числа $b_i - m$ имеют, согласно (19), отрицательные вещественные части. Положим $z_i = \exp(b_i - m)$. Имеем

$$|z_i| < 1, \quad i = 2, \ldots, N \tag{20}$$

Из теории функций от матриц (см. [**?**]) известно, что числа z_i будут характеристическими числами матрицы $\exp(A - mI)$. Жорданова форма матрицы $\exp((A - mI)t)$ имеет вид

$$\exp((A - mI)t) = T^{-1} diag(J_0, J_1, \ldots, J_L)T \tag{21}$$

Здесь T – матрица, не зависящая от t, $J_0 = (1)$ – жорданова клетка первого порядка, а $J_i, \quad i > 0$ – жорданова клетка, построенная по некоторому $z_j^t, \quad j > 1$. Из (20) теперь вытекает, что матрица $\exp(t(A - mI)a)$ стремится к матрице ранга 1, когда $t \to \infty$, поскольку все клетки $J_i, \quad i > 0$ стремятся к нулевым матрицам. Вектор $\mathbf{Q}$ останется левым собственным вектором и для матрицы $exp((A - mI)t)$ и отвечает собственному значению 1, поэтому он будет собственным вектором и для предельной матрицы. С другой стороны, матрица $exp((A - mI)t)$ будет стохастической, поэтому и предельная матрица будет тоже стохастической. Это означает, что все строки предельной матрицы совпадают с вектором $\mathbf{Q}$. Теперь из (18) следует, что

$$\mathbf{P}(t) \to \mathbf{Q}, \quad t \to \infty$$

то есть предельное распределение не зависит от начального распределения вероятностей $\mathbf{P}(\mathbf{0})$.[**?**]. Содержательно вектор $\mathbf{Q}$ представляет вероятности нахождения системы в каждом состоянии, когда время стремится к бесконечности, а сам вектор

называется финальным вектором для соответствующего марковского процесса. Обозначим через F_Q матрицу, все строки которой совпадают с вектором $\mathbf{Q}$. По любому числу ϵ можно найти такое число q, что

$$|| \exp(a(A - mI)t) - F_Q|| < \epsilon,\ t > q$$

Определяя состояния генератора с шагом q, получаем распределение вероятностей состояний близкое к финальному с заданной точностью. Это позволяет дать количественную оценку "независимости" полученного отсчета от предыдущего. Зная явный вид матрицы A, можно получить и оценку для q. Ниже будет приведен пример получения такой оценки.

1.11.1 Примеры вычисления финальных векторов для нелинейных схем

Все вычисления в данном пункте проведены с помощью пакета математических программ SciLab [**?**]. Вернемся к схеме, изображенной на Рис.4. Определим следующим образом булевы функции, реализуемые схемой. Пусть $i_0, \ldots, i_7$ - произвольное множество из чисел $i_k \in [0, 7]$. Каждое число $k \in [0, 7]$ в двоичной форме представимо тремя битами. Когда эти биты поданы на вход схемы, на выходе появляются биты, отвечающие числу i_k. Например, если $i_2 = 4$, то при подаче на вход схемы вектора $\langle 0, 1, 0\rangle$, на выходах появится вектор $\langle 1, 0, 0\rangle$. Очевидно, что любая комбинационная схема с тремя входами и тремя выходами может быть задана последовательностью $i_0, \ldots, i_7$. Предполагается, что выполнены все условия, наложенные на схему, указанные выше. В первом примере последовательность имеет вид $1, 2, 3, 4, 5, 6, 7, 0$. В этом случае матрица

$$A_1 = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Непосредственной проверкой можем убедиться, что элементы матрицы $(I+A_1)^5$ положительны, следовательно, это неразложимая матрица. В силу симметричности матрицы A_1, вектор $\mathbf{Q} = \langle 1, 1, 1, 1, 1, 1, 1, 1\rangle/8$. Это означает, что финальная вероятность каждого состояния будет одной и той же. В следующем примере последовательность

имеет вид $1,3,5,7,6,4,2,0$. Имеем

$$A_2 = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Для отыскания финального вектора в SciLab сначала вводим матрицу A_2, после чего выполняем команду

```
[a,b]=spec(A2')
```

Сначала будет напечатана диагональная матрица b, на диагонали которой находятся характеристические числа матрицы. Столбцы матрицы a есть собственные векторы матрицы A_2^T (знак $'$ означает транспонирование матрицы в SciLab), то есть получаем собственные векторы-строки исходной матрицы. Тот вектор, который будет отвечать собственному значению m и будет финальным вектором. Он равен $\langle 0.0833, 0.0833, 0.0833, 0.2500, 0.0833, 0.0833, 0.2500, 0.0833\rangle$. Практическое значение имеют не вероятности отдельных состояний, а вероятности появления 0 или 1 на отдельном выходе. Эти вероятности могут быть найдены по вероятностям появлений состояний из финального вектора путем суммирования вероятностей состояний, имеющих 0 или 1 в одной позиции. Например, найдем вероятность появления 0 на первом выходе. Для этого надо суммировать финальные вероятности состояний $\langle 0,0,0\rangle, \langle 0,0,1\rangle, \langle 0,1,0\rangle, \langle 0,1,1\rangle$, то есть вероятности состояний с номерами 0,1,2,3. Нетрудно видеть, что эта сумма равна 0.5. Аналогичный результат получается и для третьего выхода. С другой стороны, для подсчета вероятности появления 0 на втором выходе, надо суммировать финальные вероятности состояний с номерами 0,1,4,5. Теперь эта сумм равна $\frac{1}{3}$. Еще одни пример, когда последовательность выбрана в виде $2,4,6,7,5,3,1,0$. Финальный вектор в этом случае имеет вид $\langle 0.0811, 0.0811, 0.1892, 0.1351, 0.1081, 0.1622, 0.1081, 0.1351\rangle$. Здесь вероятность 0 на первом выходе равна 0.4865, вероятность 0 на втором выходе равна 0.4324, вероятность 0 на третьем выходе равна 0.4865.

Следующий пример относится к схеме, представленной на Рис.1.11.1. Здесь изображена кольцевая схема, составленная из двух схем, рассмотренных выше. Для первой схемы последовательность равна $1,2,3,4,4,3,2,1$, а для второй схемы она равна $1,3,5,7,6,4,2,0$. В этом случае схема имеет 64 состояния. Каждое состояние есть двоичный вектор длины 6, в котором первые 3 компонента - выходы первой схемы, а оставшиеся 3 компонента - выходы второй схемы. Выбор множеств обусловлен необходимостью обеспечить неразложимость матрицы A. Приведем вероятности 0 на выходах первой схемы. Это 0.7652, 0.5369, 0.4472; вероятность появления 0 на

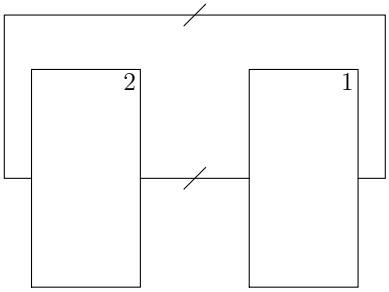

Рис. 5: Кольцевое соединение двух схем

выходе второй схемы равны 0.4159, 0.4117, 0.2348. Применение генераторов кольцевой структуры позволяет использовать много вариантов соединений схем друг с другом, не меняя самих схем. Это свойство может оказаться полезным при создании перестраиваемых генераторов криптографических ключей Одной из нерешенных проблем остается метод выбора компонентов и их соединений для обеспечения неразложимости матрицы переходов A. Каждый раз приходится проверять ее, исходя из определения.

1.11.2 Оценка близости текущих вероятностей к финальным

Матрица A по текущей схеме строится достаточно просто. Ограничимся случаем, когда в пространстве существует базис из собственных векторов матрицы A. Случай произвольной жордановой формы рассматривается аналогично, хотя требует более громоздких вычислений. Зная вид этой матрицы можно получить оценку нормы разности

$$|| \exp(a(A - mI)t) - F_Q||$$

На примере матрицы A_2 покажем, как это можно сделать. Без ограничения общности можно считать $a = 1$. Напомним, что характеристические числа обозначались символами $b_k, b_1 = 3$. Прямым вычислением находим, что $\max_{k>1} Re(b_k) = 2.4196$. Собственный вектор $\mathbf{Q}$, отвечающий собственному значению 3, был найден выше. Вычитая из всех характеристических чисел 3, получим, что в матрице $A_2 - 3I$ одно характеристическое число нулевое, а наибольшая вещественная часть остальных чисел равна -0.5804. Следовательно, среди характеристических чисел матрицы $\exp(A_2 - 3I)$ одно число равно 1, а наибольший модуль оставшихся чисел равен $d = \exp(-0.5804) = 0.55597$. В данном примере матрица A_2 имеет простой спектр, поэтому в пространстве существует базис из собственных векторов этой матрицы, а соотношение (21) принимает вид

$$A_2 = T^{-1} diag(b_1, b_2, \ldots, b_8)T,$$

где T – матрица, столбцы которой есть собственные векторы матрицы A_2. Последнее

равенство перепишем в следующей форме

$$A_2 = T^{-1}diag(b_1, 0, \ldots, 0)T + T^{-1}diag(0, b_2, \ldots, 0)T + \cdots + T^{-1}diag(0, 0, \ldots, b_8)T.$$

Вводя обозначение $B_k = T^{-1}diag(0, \ldots, b_k, 0, \ldots, 0)T$, перепишем предыдущее выражение в виде

$$A_2 = \sum_{k=1}^{8} b_k B_k$$

Это равенство известно как спектральное разложение матрицы [?]. Теперь

$$\exp(A_2 - 3I) = F_Q + \sum_{k=2}^{8} z_k B_k$$

где матрица F_Q была определена выше. Поскольку после возведения матрицы в целую степень q ее характеристические числа возводятся в ту же степень, а собственные векторы при этом не меняются, получаем

$$\exp((A_2 - 3I)r) = F_Q + \sum_{k=2}^{8} z_k^r B_k \tag{22}$$

или

$$||\exp((A_2 - 3I)r) - F_Q|| \leq \sum_{k=2}^{8} |z_k|^r ||B_k||$$

Фактически, основным параметром, определяющим скорость установления, является число d, найденное выше. Чем меньше значение этого параметра, тем быстрее происходит процесс установления финального распределения.

1.12 Генератор случайных чисел на основе сумматоров по модулю два

1.12.1 Основные определения

В предыдущем пункте был изложен общий подход к теории генераторов на основе комбинационных схем, работающих в режиме "дребезжания". В данном параграфе будет рассмотрен частный случай, когда комбинационная схема состоит из сумматоров по модулю два. Исторически именно эти схемы были впервые предложены и рассмотрены в связи с созданием генераторов случайных чисел в работе [?]. Подробное изложение вопросов, связанных со схемной реализацией таких устройств, представлено в [?]. В данном пункте остановимся на особенностях теории функционирования подобных генераторов [?]. Рассмотрим схему, представленную на Рис. 6 На свободный вход сумматора с номером 3 подается постоянный сигнал 1. Согласно подходу, изложенному выше, состояние схемы в момент времени t задается вектором $\mathbf{S(t)} = \langle y_1, y_2, y_3 \rangle^T$. Очевидно, что состояние генератора будет все время меняться.

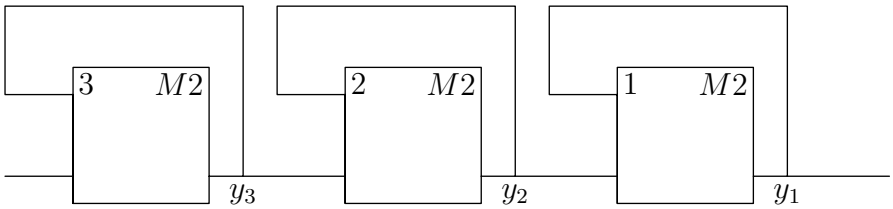

Рис. 6: Пример генератора, составленного из сумматоров по модулю два

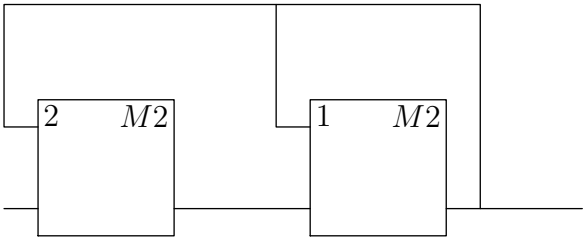

Рис. 7: Пример схемы со стабильными состояниями

1.12.2 Математическая модель

Уточним математическую модель устройства, рассмотренную ранее, в случае схемы, составленной из сумматоров по модулю 2. В дальнейшем будет говорить просто о сумматорах. В общем случае схема состоит из произвольного количества сумматоров, выходы которых соединены с входами других сумматоров или тех же самых сумматоров; сигнал с выхода одного сумматора может подаваться на входы нескольких устройств; на часть входов могут подаваться постоянные сигналы. Теперь предположения, относящиеся к общим принципам функционирования подобных устройств, выглядят следующим образом

1. Время срабатывания каждого сумматора меняется согласно экспоненциальному закону с одним и тем же параметром

2. В любой момент времени может сработать только один сумматор

3. Срабатывания сумматоров являются независимыми случайными величинами

Система уравнений типа Эрланга, описывающая динамику генератора, остается той же самой. В этом плане никаких новых эффектов, связанных с ограничениями на вид изучаемых комбинационных схем, не наблюдается. То же самое относится и к оценке времени установления генератора. Все особенности проявляются, когда переходят к вопросу о существовании стационарных состояний. Рассмотрим схему, представленную на Рис.7. На свободный вход схемы с номером 2 подан единичный сигнал. Нетрудно видеть, что состояние $\langle 1, 0 \rangle^T$ будет стабильным для устройства — из этого

состояния устройство без внешнего воздействия выйти не может. Очевидно, существование стабильных состояний в схеме является нежелательным моментом. Формально, существование таких состояний легко выявить по матрице A. Состояние с номером i будет стабильным тогда и только тогда, когда в строке матрицы с этим номером лишь элемент $A[i|i]$ отличен от нуля. Однако, если комбинационная схема имеет n выходов, матрица A имеет размер $2^n \times 2^n$ и становится мало пригодной для теоретического исследования. В случае схемы, составленной из сумматоров, существует более простой способ для выявления таких состояний.

1.12.3 Стабильные и частично стабильные состояния схемы, составленной из сумматоров

При изложении этого пункта будем следовать работе [?]. Кроме стабильных состояний, о которых шла речь выше, устройство может обладать частично стабильными состояниями. Если генератор попадает в такое состояние, то в дальнейшем выходы некоторых сумматоров остаются неизменными, хотя само состояние стабильным не будет. Очевидно, что существование таких состояний ухудшает качество генератора. Если наличие стабильных состояний легко выявляется по матрице A, то доказательство отсутствия частично стабильных состояний в схеме решается более сложно. Перенумеруем все сумматоры целыми числами от 1 до n. На свободные входы сумматоров поступают постоянные сигналы. Существование сумматора, на оба входа которого поступают постоянные сигналы, не имеет смысла. Если постоянный сигнал поступает на вход сумматора с номером k, то этот сигнал обозначим через b_k. Выход сумматора с номером k равен y_k, а состояние генератора в момент времени t есть вектор, состоящий из выходов всех сумматоров, $\mathbf{S(t)} = \langle y_1, \ldots, y_n \rangle^T$.

1.12.4 Альтернативный способ описания структуры генератора

Воспользуемся линейностью компонентов комбинационной схемы. Это дает альтернативный способ описания структуры генератора. Напомним, что все арифметические операции выполняются над полем $GF(2)$.
Сигнал y_i на выходе сумматора с номером i определяется значениями на входах, которые порождаются сумматорами, и некоторыми постоянными сигналами. В результате срабатывания сумматора с номером i может измениться лишь сигнал y_i. На входы этого сумматора могут поступать сигналы с сумматоров с номерами p и q либо сигнал с сумматора с номером p и постоянный сигнал b_i. Исключается возможность $p = q$, поскольку выход сумматора с номером i в этом случае окажется нулевым. Если сумматор с номером i не имеет свободных входов, полагаем $b_i = 0$. В результате срабатывания в первом случае значение y_i заменится на $y_p \oplus y_q \oplus b_i$. а во втором — на $y_p \oplus b_i$. Определим вектор $\mathbf{B} = \langle b_1, b_2, \ldots, b_n \rangle^T$ и матрицу L размера $n \times n$ следующим образом: в строке с номером i в первом случае $L[i|p] = L[i|q] = 1$, а остальные элементы в этой строке нулевые, а во втором случае только элемент $L[i|p] = 1$, а остальные элементы строки нулевые. Обратим внимание, что имеется дополнительное ограничение на элементы матрицы L и вектора $\mathbf{B}$, которое всегда

считается выполненным — если в строке $L[i|*]$ два ненулевых элемента, то $b_i = 0$. Изменение состояния в результате срабатывания сумматора с номером i определяется равенством

$$y_i' = L[i|*]\mathbf{S} \oplus b_i \tag{23}$$

Другими словами, матрица L и вектор $\mathbf{B}$ определяют структуру схемы и ее функционирование. В качестве примера рассмотрим схему на рис. 6. Для этого генератора матрицы L и $\mathbf{B}$ имеют вид

$$L = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Поскольку дальнейшие результаты формулируются в терминах строк матрицы L, введем для этих строк специальные обозначения – $\lambda_i = L[i|*]$. В этих обозначениях

$$L = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \cdots \\ \lambda_n \end{pmatrix}$$

Матрицу L назовем структурной матрицей генератора.

1.12.5 Стабильные состояния

Легко видеть, что при нулевом векторе $\mathbf{B}$ нулевое состояние всегда является стабильным. Интерес представляет ситуация, когда этот вектор отличен от нулевого, что и будет предполагаться в дальнейшем.

Предложение 3 *Пусть*

$$D = L \oplus I = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \cdots \\ \lambda_n \end{pmatrix} \oplus I \quad , \bar{D} = \begin{pmatrix} D[1|*], & b_1 \\ D[2|*], & b_2 \\ \cdots & \cdots \\ D[n|*], & b_n \end{pmatrix},$$

где I – единичная матрица. Тогда генератор обладает стабильными состояниями тогда и только тогда, когда

$$\mathrm{rank}(D) = \mathrm{rank}(\bar{D}), \tag{24}$$

где $\mathrm{rank}(D)$ *означает ранг матрицы D.*

Доказательство. Согласно (23), состояние $\mathbf{S}$ будет стабильным тогда и только тогда, когда

$$y_i = \lambda_i \mathbf{S} \oplus b_i, \quad i = 1, \ldots, n$$

В матричной форме это условие перепишется в виде

$$\mathbf{S} = L\mathbf{S} \oplus \mathbf{B}. \tag{25}$$

Учитывая то, что все операции осуществляются в поле $GF(2)$, запишем равенство (25) в форме

$$(I \oplus L)\mathbf{S} = \mathbf{B}$$

Другими словами, вектор $\mathbf{S}$ является решением неоднородной системы. Для того, чтобы такая система была совместной, согласно теореме Кронекера-Капелли необходимо и достаточно выполнения условия (24).

1.12.6 Частично стабильные состояния

Согласно Предложению 3, выполнение неравенства $\mathrm{rank}(D) < \mathrm{rank}(\bar{D})$ гарантирует отсутствие стабильных состояний. В то же время возможна ситуация, когда состояние не является стабильным, но при этом остаются постоянными выходы некоторых сумматоров, то есть состояние является частично стабильным. Пусть в частично стабильном состоянии $\mathbf{S} = \langle y_1, \ldots, y_n \rangle^T$ на выходах сумматоров с номерами $i_1, \ldots, i_k, \quad 0 < k < n$, сигналы не меняются в процессе работы генератора. Поскольку нумерация сумматоров является произвольной, можем считать, что в процессе работы генератора сигналы на выходах сумматоров с номерами $i, \quad i = 1, \ldots, k$ не меняются. Частично стабильное состояние представим в виде $\mathbf{S} = \langle \mathbf{S_1}, \mathbf{S_2} \rangle^T$, где $\mathbf{S_1} = \langle y_1, \ldots, y_k \rangle$, $\mathbf{S_2} = \langle y_{k+1}, \ldots, y_n \rangle$.
Согласно сделанным предположениям, имеют место равенства

$$\lambda_i \mathbf{S} \oplus b_i = y_i, i = 1, \ldots, k \tag{26}$$

при любых изменениях в компонентах вектора $\mathbf{S_2}$. Положим $\epsilon_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T$, где 1 занимает позицию с номером i. Изменение компоненты с номером $j, k < j < n$, на противоположный не должно влиять на компоненту с номером $i, 0 < i \leq k$. Указанное изменение реализуется заменой вектора $\mathbf{S}$ на $\mathbf{S} \oplus \epsilon_j$. Из (26) вытекает, что

$$\lambda_i \epsilon_j = 0, \quad j = k+1, \ldots, n; i = 1, \ldots, k. \tag{27}$$

Условие (27) означает, что при указанной нумерации сумматоров

$$L = \begin{pmatrix} C_1 & 0 \\ C_2 & C_3 \end{pmatrix},$$

где C_1 есть $k \times k$ матрица. То есть, матрица оказывается разложимой.

Предложение 4 *Для того, чтобы генератор обладал частично стабильными состояниями необходимо выполнение равенств (26), из которых следует, что структурная матрица генератора является разложимой.*

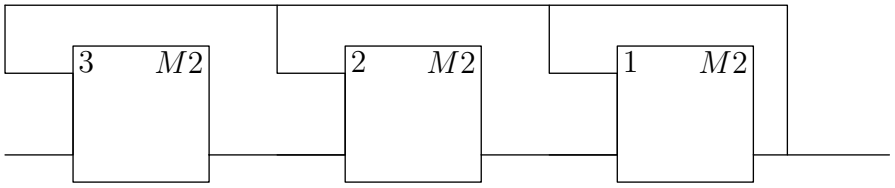

Рис. 8: Пример схемы с глобальной обратной связью

Итак, условие разложимости структурной матрицы является необходимым условием для существования частично стабильных состояний генератора. Матрица L будет неразложимой тогда и только тогда, когда все элементы матрицы $(I + L)^{n-1}$ будут положительны (при вычислении степени матрицы все операции осуществляются в поле вещественных чисел). Это дает простой способ проверки неразложимости матрицы переходов.

Разложимость матрицы L обеспечивает отсутствие влияния срабатывания сумматоров с номерами $k + 1, \ldots, n - 1$ на выходы сумматоров с номерами $i = 1, \ldots, k$. Однако, это условие не является достаточным для частичной стабильности состояния, поскольку не учитывается влияние срабатывания сумматоров с номерами $i = 1, \ldots, k$ на данное состояние.

1.12.7 Примеры

В приведенных выше примерах каждый сумматор имел ровно два входа, поэтому структурная матрица генератора имела не более двух единиц в каждой строке. На самом деле, это ограничение является несущественным, можно рассматривать сумматоры с числом входов больше, чем два, поэтому число единиц в каждой строке матрицы переходов может быть произвольным.

В качестве иллюстрации рассмотрим ситуацию со стабильными состояниями для схемы на Рис. 8. На свободный вход сумматора 3 подан единичный сигнал. Для этой схемы

$$L = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \bar{D} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Нетрудно видеть, что $\mathrm{rank}(D) = 2$ и $\mathrm{rank}(\bar{D}) = 3$ над полем $GF(2)$, и в схеме отсутствуют стабильные состояния. Над полем вещественных чисел

$$D^2 = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 1 & 1 & 1 \end{pmatrix}.$$

Это означает, что структурная матрица является неразложимой, поэтому в схеме отсутствуют частично стабильные состояния. В данном случае справедливость полученных утверждений можно проверить непосредственно. Более сложный пример

представляет кольцевая схема, состоящая из n сумматоров, когда на один вход сумматора с номером i поступает сигнал с сумматора с номером $i+1, i = 1, \ldots, n-1$, а на вход последнего сумматора поступает сигнал с первого сумматора. На второй вход каждого сумматора поступает либо постоянный сигнал, либо выход любого сумматора. Легко проверить, что матрица перестановки

$$C = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

является неразложимой. Структурная матрица L генератора получается добавлением некоторого числа единиц в строки матрицы C, поэтому матрица L также будет неразложимой. Это означает, что такая схема не может иметь частично стабильных состояний. В частности, рассмотрим схему, в которой $L = C$, то есть на один из входов каждого сумматора подается постоянный сигнал. Матрица $D = L \oplus I$ имеет в каждой строке две единицы, поэтому сумма всех столбцов матрицы есть нулевой вектор. Это означает, что rank(D) < n. Выбрав произвольный вектор $\mathbf{B}$ с нечетным числом единиц, получим, что rank(D) < rank($\bar{\text{D}}$), поскольку такой вектор $\mathbf{B}$ нельзя получить в виде линейной комбинации столбцов, в каждом из которых четное число единиц. Полученная схему не будет иметь как стабильных, так и частично стабильных состояний.

Другой крайний случай – когда схема не имеет глобальной обратной связи (пример такой схемы для $n = 3$ представлен на рис. 9). Для этой схемы

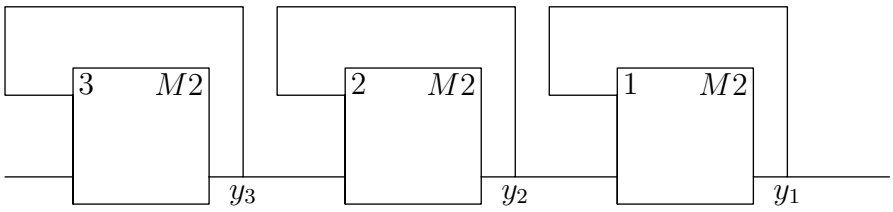

Рис. 9: Пример генератора с локальными обратными связями

$$L = \begin{pmatrix} 1 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

В этом случае матрица

$$D = L \oplus I = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Нетрудно проверить, что $\mathrm{rank}(D) = n-1,\ \mathrm{rank}(\bar{D}) = n$, поэтому схема не имеет стабильных состояний. Матрица L будет разложимой, поскольку прибавив к ней единичную матрицу, получим треугольную матрицу, которая при возведении в произвольную степень останется треугольной матрицей. С другой стороны, для этой схемы не существует частично стабильных состояний. Действительно, для $i < n$ уравнение (26) принимает форму

$$y_i \oplus y_{i+1} = y_i.$$

Отсюда следует, что $y_{i+1} = 0$, поэтому из стабильности сигнала y_i следует стабильность сигнала y_{i+1}. В то же время, сигнал y_n не может быть постоянным, поскольку $y'_n = y_n \oplus 1$.
Рассмотрим пример схемы с частично стабильными состояниями. Пусть

$$L = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Легко видеть, что $\mathrm{rank}(D) = 3$. Аналогом уравнений (27) в этом случае являются уравнения

$$\lambda_i \epsilon_j = 0,\ i = 1,4; j = 2,3.$$

Это означает, что выполнены необходимые условия для существования состояния со стабильными битами в позициях 1 и 4. Для выяснения достаточности этих условий надо рассмотреть уравнения (26):

$$\lambda_i \mathbf{B} = y_i \oplus b_i,\ i = 1,4.$$

В данной ситуации эти уравнения имеют решения для любых значений $b_1, \ldots, b_4$. Выберем эти значения таким образом, чтобы было выполнено неравенство $rank(D) < rank(\bar{D})$. Достаточно положить их равными $1,0,0,0$. В этом случае не будет стабильных состояний, но состояние $\langle 1, *, *, 1\rangle^T$ будет частично стабильным, поскольку не меняются биты в позициях 1 и 4.

1.13 Генератор случайных чисел на основе трехзначной логики

Увеличение производительности цифровых устройств является одной из основных задач современной схемотехники. Достигнутая к настоящему времени тактовая частота близка к предельно возможной. Дальнейшее повышение производительности осуществляются либо за счет распараллеливания вычислений либо путем применения устройств, работающих в k-значной логике. Следует отметить, что на заре развития вычислительной техники существовали компьютеры работающие на основе трехзначной логики. Здесь, прежде всего, следует упомянуть Н.П. Брусенцова и

его машину "Сетунь". Впоследствии интерес к таким устройствам упал в связи с производством стандартных двоичных чипов, реализующих все необходимые функции. В последнее время созданы простые физические устройства, реализующие трехзначную логику (см. [?]), что пробудило интерес к этим схемам и стимулирует разработку полезных физических приборов, работающих в трехзначной логике.
Ранее было дано математическое описание физических генераторов на основе двоичной логики. Оказалось, что аналогичный подход годится и для модели генератора, работающего в троичной логике. В его основе лежит специальная комбинационная схема трехзначной логики, работающая в режиме дребезжания. Такой генератор обладает рядом интересных свойств, поэтому дальнейшее развитие схемотехники позволит найти практическое применение для этих генераторов. В частности, они могут быть использованы для генерации криптографических ключей. Изложение данного пункта основано на работе [?].

1.13.1 Пример генератора

В качестве иллюстрации рассмотрим следующий пример схемы. Генератор построен по кольцевому принципу. Он состоит из одинаковых комбинационных схем (блоков), соединенных в кольцо. Каждый блок имеет два входа и один выход. Пример генератора из трех блоков представлен на Рис.10. Способ соединения произвольного

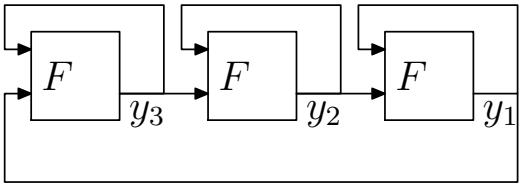

Рис. 10: Пример генератора тернарных последовательностей

числа блоков следует из этого рисунка очевидным образом. Здесь символом F обозначен упомянутый блок, а генерируемый сигнал снимается с выхода любого из блоков. Сигнал является троичным, благодаря чему увеличивается производительность устройства по сравнению с двоичным аналогом, работающим с той же скоростью.

1.13.2 Математическая модель генератора

При создании указанных генераторов возникают следующие проблемы:

1. возможность перехода генератора в стабильное состояние;

2. обоснование нужных статистических свойств сгенерированных символов.

Ниже будет показано, что при надлежащем выборе блока F и способа соединения блоков между собой генератор не имеет стабильных состояний. Что касается статистических свойств генерируемой последовательности, то о них можно говорить лишь

после того, как будут выбраны математическая модель функционирования отдельных блоков и способ съема сигнала. Естественными требованиями являются равномерность распределения выходного сигнала и независимость снимаемых сигналов. В этом случае появляется возможность преобразования выходного сигнала в сигнал с произвольным распределением. Общий подход к исследованию генератора, составленного из нелинейных блоков, представлен в предыдущей главе, однако применение трехзначной логики вносит некоторые упрощения в описание ситуации. Каждый из блоков реализует некоторую функцию $c = F(a, b)$, $a, b, c \in \{0, 1, 2\}$. При изменении входных сигналов блок срабатывает, реализуя функцию F. Относительно срабатывания блоков сделаны предположения аналогичные ограничениям, использованным при моделировании двоичных схем:

1. время срабатывания блока является случайной величиной с экспоненциальным распределением.

2. срабатывания отдельных блоков являются независимыми событиями, причем никакие два блока не могут сработать одновременно.

Ради простоты в дальнейшем будем предполагать, что параметр экспоненциального распределения равен 1. Перенумеруем блоки генератора числами от 1 до n. Состоянием генератора в момент времени t назовем вектор $\mathbf{S}(t) = \langle y_1, \ldots, y_n \rangle^T$, компонента которого y_k есть сигнал на выходе блока с номером k в момент времени t. В отличие от двоичного случая, $y_k \in \{0, 1, 2\}$. Если генератор содержит n блоков, то число его состояний равно $m = 3^n$. Благодаря сделанным предположениям функционирование генератора описывается уравнениями Эрланга [**?**]. Система строится аналогично двоичному случаю, но для полноты изложения приведем вывод уравнений. Перенумеруем все состояния генератора числами от 1 до m. Пусть $\mathbf{S}_q$ — состояние с номером q, а $P_q(t)$ — вероятность того, что в момент времени t генератор находится в состоянии $\mathbf{S}_q$. Обозначим через $i_1, i_2, \ldots, i_r$ — все номера состояний, свои для каждого q, из которых можно попасть в состояние $\mathbf{S}_q$ в результате срабатывания только одного блока. Вероятность того, что через момент Δt генератор окажется в состоянии $\mathbf{S}_q$, складывается из вероятности того, что генератор находился в этом состоянии прежде и ни один из n блоков не сработал и из вероятностей перейти в состояние $\mathbf{S}_q$ из одного из состояний с номерами $i_1, i_2, \ldots, i_r$ в результате срабатывания только одного блока. Учитывая только слагаемые первой степени по Δt, получим, что вероятность срабатывания одного блока равна Δt, а вероятность того, что ни один блок на сработает равна $1 - n\Delta t$. Теперь

$$P_q(t + \Delta t) = (1 - n\Delta t)P_q(t) + \sum_{k=1}^{r} P_{i_k}\Delta t,$$

откуда, деля на Δt и переходя к пределу при $\Delta t \to 0$, получим

$$\frac{dP_q(t)}{dt} = -nP_N(t) + \sum_{k=1}^{r} P_{i_k}(t). \tag{28}$$

Функционирование системы полностью описывается с помощью решения системы (28), однако размер матрицы этой системы быстро растет с увеличением числа блоков, что делает затруднительным исследование особенностей поведения системы. Ниже будет показано, что используя дополнительные соображения, можно сделать выводы о свойствах решения, не решая саму систему.

1.13.3 Выбор функции F

При выводе уравнения (28) не делалось никаких предположений о виде функции F. В данном пункте будут приведены соображения по поводу выбора этой функции. Прежде всего, нужно гарантировать отсутствие стационарных состояний генератора. Предположим, что функция F обладает следующим свойством:

$$c = F(a,b), \quad \forall (a,b) \quad c \neq a,b. \tag{29}$$

Из условия (29) следует, что при срабатывании любого блока состояние генератора изменится при любом соединении блоков между собой. Таким образом, данное условие исключает наличие стационарных состояний. Перечислим все функции, обладающие свойством (29). Значение $F(a,b)$ определено однозначно, если $a \neq b$, поэтому $F(a,b) = F(b,a)$. Это означает, что достаточно определить функцию лишь для совпадающих аргументов. Если σ — произвольная перестановка чисел $0,1,2$, то функции $F(a,b)$ и $\sigma(F(\sigma(a),\sigma(b))$ будем считать неразличимыми. Действительно, для наших целей не играет роли, как будет обозначен тот или иной элемент троичной логики. Отсюда следует, что существуют лишь две существенно разные функции, обладающие свойством (29):

	$F(0,0)$	$F(1,1)$	$F(2,2)$
F_1	1	2	0
F_2	1	2	1

Изучаемый генератор предназначен для генерации последовательностей, в которых каждый из элементов появляется с одной и той же вероятностью. В этой связи далее в качестве функции F будем использовать только F_1. В дальнейшем будем применять символ F для обозначения этой функции.

Теперь надо определить способ соединения блоков между собой. Остается открытым вопрос о связи топологии соединения блоков со свойствами генератора. В данном пункте будет изучен лишь один из вариантов соединения, представленный на Рис.10. Достоинством указанной схемы является равноправность всех выходов блоков и одинаковая электрическая нагрузка на выходе каждого блока. Последнее условие, которое носит технологический характер, важно и с точки зрения адекватности математической модели. Время срабатывания физического блока может зависеть от того, на сколько входов будет подан сигнал. В этой связи, равноправность всех блоков в предложенной схеме становится существенным элементом. В дальнейшем будет показано, что схема обладает свойством «забывания» начального состояния, поэтому, в силу отмеченной симметрии, на выходе любого блока при снятии сигнала через

достаточно большой интервал времени t_0 статистические свойства сигнала будут одними и теми же. Более того, функция F обладает тем свойством, что любое значение на выходе появляется одинаковое количество раз, когда аргументы пробегают всю область определения функции. Интуитивно ясно, что в силу этого обстоятельства на выходе каждого блока генерируется сигнал с равномерным распределением. Далее будет доказана справедливость этого предположения.

1.13.4 Матрица переходов генератора

Для обоснования статистических свойств снимаемого сигнала необходимо изучить свойства матрицы A переходов генератора. Это матрица размера $m \times m$ $m = 3^n$. Напомним, что матрица состоит из нулей и единиц, причем $A[i|k] = 1$ тогда и только тогда, когда при срабатывании какого-либо блока генератор переходит из состояния с номером i в состояние с номером k. Рассмотрим произвольное состояние

$$\mathbf{S} = \langle y_1, \ldots, y_k, \ldots, y_N \rangle^T. \tag{30}$$

В силу свойства (29), в результате срабатывания любого из n блоков состояние генератора изменится, причем все получившиеся состояния будут разными. Это означает, что каждая строка матрицы A имеет ровно n единиц.

Предложение 5 *Состояния (30), в которых все сигналы равны между собой, при указанных выборе функции F и способе соединения блоков недостижимы из других состояний генератора.*

Доказательство
Рассмотрим состояние $\mathbf{S_0} = \langle 0, \ldots, 0 \rangle^T$. Если из некоторого состояния $\mathbf{S_1}$ возможен переход в состояние $\mathbf{S_0}$ в результате срабатывания одного блока, то все компоненты вектора $\mathbf{S_1}$, кроме одной, равны 0. Легко видеть, что после срабатывания любого блока, в силу (29), переход в состояние $\mathbf{S_0}$ невозможен. Поскольку в рассматриваемой схеме все троичные значения равноправны, аналогичные утверждения справедливы для векторов $\langle 1, \ldots, 1 \rangle^T$ и $\langle 2, \ldots, 2 \rangle^T$.
Из доказанного утверждения следует, что столбцы с номерами, отвечающими трем недостижимым состояниям, будут нулевыми. Удалим из A эти три строки и три столбца с указанными номерами и обозначим через A' получившуюся матрицу. Это квадратная матрица с неотрицательными элементами, и все утверждения, относящиеся к таким матрицам, представленные выше, остаются справедливыми и для этой матрицы.
Свойства генерируемой последовательности базируются на следующей теореме.

Теорема 2 *Матрица A' является неразложимой.*

Доказательство
Под множеством состояний будем понимать множество всех состояний генератора, кроме трех отмеченных недостижимых состояний. Достаточно доказать, что из любого состояния можно перейти в любое другое. Пусть $\mathbf{S_1} = \langle 1, 0, \ldots, 0 \rangle^T$. Покажем,

что из $\mathbf{S_1}$ можно перейти в любое другое состояние через несколько шагов, свое для каждого состояния. После двукратного срабатывания второго блока генератор перейдет в состояние $\langle 1,1,0,\ldots,0\rangle^T$, а затем – в состояние $\langle 1,2,0,\ldots,0\rangle^T$. Итак, доказано, что из $\mathbf{S_1}$ можно перейти в состояние $\langle 1,a,0,\ldots,0\rangle^T$, где a – любой элемент множества $L=\{0,1,2\}$. При срабатывании первого блока переходим из состояния $\mathbf{S_1}$ в состояние $\langle 2,0,0,\ldots,0\rangle^T$. После этого, как и выше, доказывается, что достигается любое состояние $\langle 2,a,0,\ldots,0\rangle$, где $a\in L$. Предположим, что уже доказана достижимость из состояния $\mathbf{S_1}$ любого состояния вида $\langle 1,a_2,a_3,\ldots,a_k,0,\ldots,0\rangle^T$ или $\langle 2,a_2,a_3,\ldots,a_k,0,\ldots,0\rangle^T$, где $a_2,a_2,\ldots,a_k$ – любые элементы множества L. Если $k<n-1$, то при срабатывании блока с номером $k+1$ из состояния $\langle 1,a_2,$ $a_3,\ldots,a_k,0,0,\ldots,0\rangle$ переходим в состояние $\langle 1,a_2,a_3,\ldots,a_k,1,0,\ldots,0\rangle$, а затем — в $\langle 1,a_2,a_3,\ldots,a_k,2,0,\ldots,0\rangle^T$. Если $k=n-1$, то при срабатывании блока с номером n из состояния $\langle 1,a_2,a_3,\ldots,a_k,0\rangle^T$ переходим в состояние $\langle 1,a_2,a_3,\ldots,a_k,2\rangle^T$, а из состояния $\langle 2,a_3,\ldots,a_k,0\rangle^T$ – в $\langle 2,a_2,a_3,\ldots,a_k,1\rangle^T$. Таким образом, доказана достижимость состояний вида $\langle a_1,\ldots,a_n\rangle^T$, где $a_1\neq a_n$ и $a_1\neq 0$. После срабатывания первого блока переходим из состояния $\langle 1,2,a_3,\ldots,a_n\rangle^T$ в состояние $\langle 0,2,a_3,\ldots,a_n,\rangle^T$, а из состояния $\langle 2,1,a_3,\ldots,a_n\rangle^T$ в состояние $\langle 0,1,a_3,\ldots,a_n,\rangle^T$. Это означает, что из состояния $\mathbf{S_1}$ достижимо любое состояние вида $\langle 0,a_2,a_3,\ldots,a_n,\rangle^T$, где $a_2\neq 0$. Продолжая очевидным образом, получаем, что достижимо любое состояние вида $\langle 0,0,\ldots,a_k,\ldots,a_n,\rangle^T$, где $a_k\neq 0, k\leq n$. Наконец, покажем достижимость состояния вида $\langle 1,\ldots,1,b_p,\ldots,b_{n-1},1\rangle^T$, где $b_p\neq 1$. Согласно предположению, достижимо состояние $\langle 2,0,\ldots,0,b_p,\ldots,b_{n-1},1\rangle^T$. После последовательного срабатывания блоков с номерами $1,2,\ldots,p-1$ получим состояние $\langle 1,\ldots,1,b_p,\ldots,b_{n-1},1\rangle^T$, поскольку $b_p=0$ или $b_p=2$. Точно также доказывается достижимость состояния вида $\langle 2,\ldots,2,b_p,\ldots,b_{n-1},2\rangle^T$, где $b_p\neq 2$. Достижимость состояния вила $\langle 0,\ldots,,b_p,\ldots,b_{n-1},0\rangle^T$, где $b_p\neq 0$, была доказана выше.

Теперь покажем, что из любого состояния $\mathbf{S}$ можно перейти в состояние $\mathbf{S_1}$. При срабатывании первого блока происходит переход из состояния $\langle 0,a_2,\ldots,a_n\rangle^T$ в состояние $\langle b,a_2,\ldots,a_n\rangle^T$, где $b=1$ или $b=2$. Это означает, что можем ограничиться состояниями, начинающимися с 1 или 2. Из состояния $\langle 1,0,\ldots,0,1\rangle^T$ после двукратного срабатывания блока с номером n получаем состояния $\langle 1,0,\ldots,0,2\rangle$, $\langle 1,0,\ldots,0,0\rangle^T$. Из состояния $\langle 2,0,\ldots,0,0\rangle^T$ после срабатывания блока с номером n получается состояние $\langle 2,0,\ldots,0,1\rangle^T$, а после срабатывания первого блока получаем $\langle 1,0,\ldots,0,1\rangle^T$. Из состояния $\langle 2,0,\ldots,0,2\rangle^T$ после срабатывания блока с номером n получается состояние $\langle 2,0,\ldots,0,0\rangle^T$.

Это означает, что состояние $\mathbf{S_1}$ достижимо из состояний вида $\langle 1,0,\ldots,0,a\rangle$, $\langle 2,0,\ldots,0,a\rangle^T$ для любых $a\in L$. Пусть уже доказана достижимость $\mathbf{S_1}$ из состояний вида $\langle 1,0,\ldots,0,b_p,\ldots,b_n\rangle^T$ для любых $b_i\in L$. Рассмотрим произвольное состояние вида $\langle 1,0,\ldots,0,b_{p-1},b_p,\ldots,b_N\rangle^T$, $b_{p-1}\neq 0$. Возможны следующие наборы значений b_{p-1},b_p : (1,2), (2,1), (2,2), когда после срабатывания блока с номером $p-1$ получаем 0 в позиции $p-1$; (1,1), когда после двукратного срабатывания блока с номером $p-1$ получаем 0 в позиции $p-1$; (2,0), (1,0) – последняя ситуация требует дополнительного рассмотрения. Рассмотрим состояние $\langle 1,0,\ldots,0,1,0,b_{p+1},\ldots,b_N\rangle^T$. При срабатывании блока с номером p в

этой позиции появится 1 или 2, что сводит эту ситуацию к предыдущему случаю. Для завершения доказательства достаточно поменять местами значения 1 и 2.

1.13.5 Статистические свойства генерируемой последовательности

Введем обозначение $B = A^T$. Согласно определению матрицы A, каждая строка матрицы B с номером i содержит 1 в позиции j тогда и только тогда, когда возможен переход из состояния с номером j в состояние с номером i в результате срабатывания одного блока. Рассмотрим более подробно систему уравнений (28). Положим $\mathbf{P}(t) = (P_1(t), \ldots, P_m(t))^T$. Указанная система может быть переписана в виде

$$\frac{d\mathbf{P}(t)}{dt} = (B - n \cdot I)\mathbf{P}(t) = D\mathbf{P}(t). \tag{31}$$

Решение данной системы имеет вид

$$\mathbf{P}(t) = \exp(Dt)\mathbf{E},$$

где $\mathbf{E}$ – произвольный стохастический вектор, определяющий начальное состояние. Матрица B имеет три нулевых строки; пусть это строки с номерами 1, 2, 3. Из (31) следует, что

$$P_k(t) = e_k \exp(-nt), \quad k \in \{1, 2, 3\}, \tag{32}$$

где $0 \le e_k \le 1$. Отсюда вытекает, что $P_k(t) \to 0$ при $t \to \infty$, $k \in \{1, 2, 3\}$. Исключим из векторов компоненты с индексами 1, 2, 3, а из матриц — строки и столбцы с этими номерами. В результате получим векторы $\mathbf{E}'$, $\mathbf{P}'(t)$, $D' = A'^T - n \cdot I'$, а решение системы (31) сведется к вычислению

$$\mathbf{P}'(t) = \exp(D't)\mathbf{E}'. \tag{33}$$

Теорема 3 *Пусть $C(t) = \exp(Dt)$. Тогда $C(t) \to C_0$ при $t \to \infty$, где C_0 – матрица с одинаковыми столбцами, равными стохастическому вектору $\mathbf{d}$, такому, что $\mathbf{d} = \langle 0, 0, 0, \mathbf{d}' \rangle^T$, $A'^T\mathbf{d}' = n\mathbf{d}'$.*

Доказательство
Из (32) вытекает, что первые три строки матрицы C_0 нулевые. Сумма элементов в каждой строке матрицы A равна n и при выбранной нумерации состояний её первые три столбца нулевые. Таким образом, матрица A'/n стохастическая, ее максимальное характеристическое число равно 1, все остальные характеристические числа имеют модули, не превосходящие 1 (см. [?] с.200), а из неразложимости этой матрицы вытекает, что 1 является простым корнем. Другими словами, если $r_1, \ldots, r_{m-3}$ — все характеристические числа матрицы A', и r_1 – максимальный по модулю вещественный корень, то $r_1 = n$, $Re(r_i) < n$, $i > 1$. По определению $D' = A'^T - n \cdot I'$, поэтому для характеристических чисел q_j этой матрицы выполнены условия $q_1 = 0$, $Re(q_i) < 0$, $i = 2, \ldots, m-3$. Характеристические числа матрицы $C'(t) = \exp(D't)$ равны $\exp(q_i t)$, поэтому модули всех характеристических чисел, кроме первого, меньше

1. Отсюда следует существование предела $C'_0 = \lim_{t\to\infty} C'(t)$, и матрица C'_0 имеет ранг 1. Если $A'^T\mathbf{d}' = n\mathbf{d}'$, то $D'\mathbf{d}'$ — нулевой вектор, а из представления матрицы $C'(t)$ в виде ряда вытекает, что $C'(t)\mathbf{d}' = \mathbf{d}'$ для любого t. Это означает, что $C'_0\mathbf{d}' = \mathbf{d}'$. Далее, $\langle 1,1,\ldots,1\rangle A'^T = n\langle 1,1,\ldots,1\rangle$, поэтому $\langle 1,1,\ldots,1\rangle D'$ — нулевой вектор и $\langle 1,1,\ldots,1\rangle C'_0 = \langle 1,1,\ldots,1\rangle$, т. е. сумма элементов в каждом столбце этой матрицы равна 1. Это замечание завершает доказательство теоремы
Вектор $\mathbf{d}'$ задает финальное распределение вероятностей состояний генератора. Из Теоремы 3 следует независимость этого распределения от начального состояния, а финальные вероятности появления 0, 1 и 2 на выходе любого блока равны 1/3. Последнее утверждение вытекает из симметричности схемы. В равновероятности появления каждого из чисел 0, 1 и 2 на выходе можно убедиться непосредственно. Например, чтобы найти вероятность появления 1 на выходе первого блока, надо выписать все состояния, у которых в троичной кодировке номера в первой позиции стоит 1. Если число блоков равно 2, то такими состояниями будут состояния с номерами 3,4 и 5. После этого суммируют финальные вероятности каждого из этих состояний. Следует, однако, заметить, что отсюда нельзя заключить, что финальные вероятности каждого из состояний генератора совпадают между собой. Они будут, вообще говоря, разными.

1.13.6 Результаты численных экспериментов

При практическом использовании разработанного генератора возникает вопрос о скорости сходимости решения уравнения (31) к финальному вектору в зависимости от числа n блоков в схеме. В качестве меры близости было выбрано среднеквадратическое отклонение δ финального вектора — собственного вектора матрицы D, отвечающего собственному значению 0, от первого столбца матрицы $\exp(Dt)$. Результаты экспериментов помещены в следующую таблицу:

Таблица Зависимость δ от n и t

$n\backslash t$	2	4	6	8	10
2	0.0095249	0.0001857	0.0000034	6.288D-08	1.141D-09
3	0.0026750	0.0000398	0.0000005	7.596D-09	1.102D-10
4	0.0014727	0.0000404	0.0000011	3.592D-08	1.113D-09
5	0.0004785	0.0000077	8.981D-08	9.856D-10	3.056D-11
6	0.0001991	0.0000055	0.0000002	6.546D-09	2.868D-10

Из приведенных результатов следует, что при любом n схема, практически, забывает свое начальное состояние при $t \geq 5$. Еще раз подчеркнем, что расчет велся для случая, когда параметр экспоненциального распределения равен 1. Для произвольного значения a этого параметра нужно заменить t на ta.