ИНСТИТУТ
ЯДЕРНОЙ ФИЗИКИ СОАН СССР

ИЯФ 42-71

М.В.Антипов

АНАЛИЗ ПРОИЗВОДЯЩИХ МНОЖИТЕЛЕЙ МУЛЬТИПЛИКАТИВНОГО ДАТЧИКА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Новосибирск

1971

Лемером /1/ в 1951 г. предложен метод вычетов (мультипликативный метод сравнения) для получения последовательности псевдослучайных чисел на ЭВМ.

Пусть заданы числа $c_0, c_1, \ldots, c_n$ и начальные числа последовательности $x_0, x_1, \ldots, x_{n-1}$, все положительные, целые и меньше некоторого M. Тогда

$$x_{n+i} \equiv c_1 x_i + c_2 x_{i-1} + \ldots + c_n x_{i+n-1} + c_0 \pmod{M}$$

будет генератором целых положительных псевдослучайных чисел. Псевдослучайное число, гипотетически равномернораспределенное в /0,1/ получается из членов последовательности X делением их на M.

В практических вычислениях используется генератор (датчик) псевдослучайных чисел вида:

$$x_{n+1} \equiv \lambda x_n \pmod{M} \quad \text{или} \qquad (1)$$

$$x_{n+1} \equiv \lambda x_n + c \pmod{M}, \qquad (2)$$

называемый мультипликативным датчиком смешанного типа.

К датчикам псевдослучайных чисел предъявляется ряд требований, которые перечислены ниже в порядке их важности.

1. <u>Наилучшее статистическое качество псевдопоследовательности</u>

Еще в 1938-1939 годах Кендалл и Бэбингтон-Смит /2-3/ для проверки качества псевдослучайной последовательности предложили систему тестов: четыре различных способа оценки случайности получающихся чисел. Большинство статей о мультипликативном датчике дают результаты проверки последовательности очередной модернизированной системой тестов /4-10/. Нельзя не отметить субъективизм в выборе системы тестов различными авторами. Так, например, Дэвис /12/ получает неплохие результаты для аддитивного датчика, в то время как другие авторы отвергают его, как заведомо плохой.

2. Максимальная длина отрезка апериодичности

Последовательность, длина которой больше отрезка апериодичности, не может быть приемлемой в статистическом отношении; однако эта величина является очень грубой верхней границей длины псевдопоследовательности, ибо зачастую можно пользоваться лишь какой-то частью отрезка апериодичности.

3. Минимальное машинное время генерации очередного псевдослучайного числа. Так как псевдослучайных чисел для большинства задач требуется все больше и больше, то это требование не является излишним. Разработка и использование аддитивного датчика /12/: $x_{n+1} = x_n + x_{n-1} \pmod M$ как раз и объясняется малым машинным временем получения x_{n+1} (одна операция типа сложения). Однако экономия машинного времени, как правило, находится в противоречии с требованием 1.

4. Минимальный объём занимаемой оперативной памяти. Это требование для датчиков, не связанных с табличным заданием, не имеет существенного значения.

Датчик на ЭВМ может быть организован при помощи следующих операций:

1. Логические операции являются минимальными перемешивающими операциями, ибо результат логической операции в i-том разряде не влияет на остальные. Кроме того, результаты операции "или" и "и" имеют различные, не равные 1/2 вероятности появления нуля или единицы (при случайных исходных). Поэтому из логических операций в датчиках можно использовать сложение по $(\mathrm{mod}\ 2)$ (поразрядное сложение).

2. Операции типа сложения обладают большим перемешивающим свойством по сравнению с логическими, так как результат операции в i-том разряде может повлиять на результат в более старшем разряде. Если перемешивающий эффект операции поразрядное сложение условно принять за единицу, то сложение будет оцениваться в 1,5. Действительно, с вероятностью 1/4 результат сложения в i-том разряде будет воздействовать на результат i-1-го, более старшего разряда, с вероятностью 1/4 . 1/2 на результат i-2-го разряда и т.д. Тогда условное число для операции типа сложения равно $1 + 1/4(1 + 1/2 + \ldots) = 1{,}5$. Операция типа сложения более подходит для организации датчика псевдослучайных чисел. Именно на её основе работает аддитивный датчик.

3. Операции типа умножения дают на двоичных машинах числа с двойным количеством разрядов. При получении чисел по $\mathrm{mod}\ 2^P$ можно из произведения выбирать средние разряды (середина квадрата, дробная часть произведения) или последние (младшие) разряды (метод вычетов). Как показано в /15/, максимальный перемешивающий эффект для умножения (в наших условных единицах) достигается при чередовании нулей и единиц одного из сомножителей и равен $(P + P-2 + P-4 + \ldots)/P \sim P/4$ условных единиц операций сложения или $P/4 \cdot 1{,}5 = 3P/8$ условных единиц операции поразрядное сложение.

При $P = 36$ по своему перемешивающему эффекту операция умножения может быть приравнена к девяти операциям сложения. Так как умножение на ЭВМ лишь в 2-3 раза занимает больше времени, чем сложение, то очевидна выгода применения операции умножения для организации датчика псевдослучайных чисел.

4. Операции (команды) управления и прочие операции иногда включаются в датчики псевдослучайных чисел, они по своему перемешивающему эффекту обычно не превосходят операций сложения, но из-за их специфичности для каждого вида ЭВМ не представляется возможным дать более точную оценку таких операций.

Таким образом, наилучшим будет датчик, использующий операцию умножения. Из нескольких видов датчиков, включающих операцию умножение, в данное работе рассматривается мультипликативный датчик сравнения по $\mathrm{mod}\ 2^P$.

II. Корреляционный коэффициент полного периода.

Пусть даны две конечные числовые последовательности $X = \{x_i\}$ и $Y = \{y_i\}$, где $i = 1, 2, \ldots, n$. Вычислены их средние значения $\overline{x} = 1/n \sum_1^n x_i$ и $\overline{y} = 1/n \sum_1^n y_i$. Одним из способов определения независимости между X и Y является вычисление коэффициента корреляции /16/:

$$\rho(X,Y) = \frac{\sum\limits_1^n (x_i - \bar{x})(y_i - \bar{y})}{\left(\sum\limits_1^n (x_i-\bar{x})^2 \sum\limits_1^n (y_i - \bar{y})^2\right)^{1/2}} \qquad (3)$$

причём ρ может изменяться в интервале / − 1,1 /. Мерой независимости последовательностей служит близость $|\rho|$ к нулю.

Покажем, что этот критерий не является достаточно эффективным. Например, пусть X и Y последовательности с периодом n, причём:

a) соответствующие члены последовательностей связаны соотношением: $y_i \equiv x_i + C \pmod M$, где M – целое, $M \geqslant n$, $0 \leqslant x_i, y_i \leqslant M-1$.

в) после нормирования последовательностей, то-есть деления членов последовательности на M имеем $0 \leqslant \frac{x_i}{M}, \frac{y_i}{M} \leqslant 1$.

c) пусть S – множество тех i, для которых $x_i + C \geqslant M$, а C таково, что для каждого $x_i \in X$ найдется такое $y_j \in Y$, что $x_i = y_j$ (последнее предложение дается для упрощения выкладок). Тогда из формулы /3/ следует: $\rho(X,Y) \sim 1 - \frac{12}{n}\sum\limits_{i\in S}\left(\frac{x_i}{M} - \frac{\bar{x}}{M}\right)$, то есть при различных C величина $\rho(X,Y)$ может изменяться от − 1/2 (при $C \sim M/2$) до 1 (при C близких к M или нулю). Можно, в частности, найти такое $C = C_0$, что $\rho(X,Y)$ будет близок к нулю. Столь большие колебания $\rho(X,Y)$ в зависимости от C заставляют осторожнее отнестись к оценке зависимости последовательностей методом корреляционного коэффициента.

Рассмотрим датчики $x_{n+1} \equiv \lambda x_n \pmod M$ и $x_{n+1} \equiv \lambda x_n + C \pmod M$. Если λ и M взаимно просты (а это всегда будет предполагаться), то введем понятие обратного датчика. <u>Определение 2.1</u>. Датчик $f(\lambda_1, C_1)$ будет обратным для датчика $f(\lambda_2, C_2)$, если последовательности, полученные датчиками, связаны соотношением: $x_i^1 = x_{n-i}^2$ для $i = 0, 1, \dots, n-1$, где n –период последовательностей.

Для датчика $x_{n+1} \equiv \lambda x_n \pmod M$ это означает, что найдется такое λ^{-1} $(\lambda\lambda^{-1} \equiv 1 \pmod M)$, что $x_{n+1}\lambda^{-1} \equiv x_n \pmod M$. Аналогично для датчика $x_{n+1} \equiv \lambda x_n + C \pmod M$ найдется λ^{-1}, а $C^{-1} \equiv \lambda^{-1}(M-C) \pmod M$.

Датчик, обратный для f, обозначим f^{-1}. Заметим, что $(f^{-1})^{-1} = f$ так как $(\lambda^{-1})^{-1} \equiv \lambda \pmod M$, а $C \equiv \lambda(M - \lambda^{-1}(M-C)) \pmod M$.

<u>Определение 2.2</u>. Датчики f и g назовем эквивалентными, если для каждой последовательности $X = \{x_i\}$ произведение корреляционных коэффициентов $\rho\{X, f(X) - g(X)\} \cdot \rho\{X, f^{-1}(X) - g(X)\} = 0$

Здесь знак минус означает, что для каждого i находится разность $\{f(x_i) - g(x_i)\} \pmod M$. Следующие шесть предложений легко получаются из определений:

1° Датчик f эквивалентен самому себе.

2° Датчик $f + C_1$ эквивалентен датчику $f + C_2$.

3° Если датчики f и g эквивалентны, то эквивалентны также датчики f^{-1} и g, f и g^{-1}, f^{-1} и g^{-1}.

4° Если датчики f и g эквивалентны, то датчики Cf и Cg также эквивалентны.

5° Если датчик f эквивалентен датчику g, а g – датчику h, то датчики f и h эквивалентны.

6° Если датчики f_1 и g_1, f_2 и g_2 эквивалентны, то осуществляется одно из двух: либо датчик $f_1 + f_2$ эквивалентен датчику $g_1 + g_2$, либо датчик $f_1^{-1} + f_2$ эквивалентен датчику $g_1 + g_2$.

Наиболее важным представляется

Следствие 2.1. Датчик $x_{i+1} \equiv \lambda x_i \pmod{M}$ эквивалентен датчикам $x_{i+1} \equiv \lambda x_i + c \pmod{M}$ и $x_{i+1} \equiv \equiv \lambda^{-1} x_i + c \pmod{M}$. Заметим, что представление датчиков в более общем виде: $x_{i+k} \equiv \lambda^k x_i \pmod{M}$ и $x_{i+k} \equiv \lambda^k x_i + \frac{c(\lambda^k - 1)}{\lambda - 1} \pmod{M}$ /11/ ($k \geq 1$) не повлияет на справедливость следствия, ибо для каждого фиксированного k величина $\frac{c(\lambda^k-1)}{\lambda-1} = C_k$ будет константой.

Многочисленные статистические проверки /4-11/, а также теоретическая оценка мультипликативного датчика /11/ позволяют утверждать, что датчик смешанного типа несколько предпочтительнее датчика несмешанного типа для одного и того-же λ. Это можно объяснить тем, что период последовательности, получаемой датчиком смешанного типа в четыре раза больше. Для больших периодов (порядка $2^{30} - 2^{40}$) можно считать, что статистические характеристики этих двух датчиков совпадают.

В дальнейшем будем рассматривать только датчик несмешанного типа:

$$x_{n+1} \equiv \lambda x_n \pmod{2^p}$$

Пусть в формуле /3/ $X = \{x_i\} = \{\lambda^i x_0\}$, а $Y = \{x_{i+k}\} = \{\lambda^{i+k} x_0\}$, то есть последовательность Y начинается с k-того члена последовательности X.

Обозначим период последовательности X через n, тогда имеем:

$$\rho(X,Y) = \frac{\sum_1^n (x_i - \bar{x})(x_{i+k} - \bar{x})}{\sum_1^n (x_i - \bar{x})^2} \tag{4}$$

В работе /4/ показано, что максимальный период для $M = 2^p$ достигается при $\lambda \equiv 3 \pmod 8$, $\lambda \equiv 5 \pmod 8$, $x_0 = 2t+1$ и равен 2^{p-2}. Тогда $\bar{x} = 2^{p-1} + \bar{\varepsilon}$, где $|\bar{\varepsilon}| \leq 2$ /15/.

Члены последовательности X расположим в порядке возрастания.

Вновь полученную последовательность обозначим X^*. Тогда для каждого i ($0 \leq i \leq 2^{p-2} - 1$) возможно такое представление: $x_i^* = 4i + \varepsilon_i$, где $-1 \leq \varepsilon_i \leq 5$.

Например, для $\lambda \equiv 5 \pmod 8$ величина ε_i - константа и равна 1, если $x_0 = 1$ или 3, если $x_0 = 7$ /15/.

Обозначим: $\lambda_k \equiv \lambda^k \pmod{2^p}$. Тогда из формулы (4) следует:

$$\rho(X,Y) = \frac{\sum_0^{2^{p-2}-1} (4i + \varepsilon_i - 2^{p-1} - \bar{\varepsilon})(\lambda_k (4i + \varepsilon_i) \pmod{2^p} - 2^{p-1} - \bar{\varepsilon})}{\sum_0^{2^{p-2}-1} (4i + \varepsilon_i - 2^{p-1} - \bar{\varepsilon})^2}$$

Рассмотрим случай $\lambda \equiv 5 \pmod 8$, тогда $\varepsilon_i = \bar{\varepsilon}$ и

$$\rho(X,Y) = \frac{\sum_0^{2^{p-2}-1} (i - 2^{p-3})(\lambda_k (4i + \bar{\varepsilon}) \pmod{2^p} - 2^{p-1})}{4 \sum_0^{2^{p-2}-1} (i - 2^{p-3})^2} =$$

$$\frac{12}{(2^{p-3})8 + 2^{p-1}} \sum_{i=0}^{2^{p-2}-1} (i - 2^{p-3})\left(\left(\lambda_k i + \frac{\lambda_k \bar{\varepsilon}}{4}\right) \pmod{2^{p-2}} - 2^{p-3}\right).$$

Согласно предложению 2° об эквивалентности двух датчиков, датчик $z_{i+1} \equiv (\lambda_k z_i + \lambda_k \bar{\varepsilon}/4) \pmod{2^{p-2}}$ эквивалентен датчику $z_{i+1} \equiv \lambda_k z_i \pmod{2^{p-2}}$. Тогда после замены датчиков и некоторых преобразований получаем:

$$\rho(X,Y) = \left(\frac{12}{(2^{p-2})^3} - \frac{24}{(2^{p-2})^5}\right) \sum_{i=0}^{2^{p-2}-1} (i - 2^{p-3})(\lambda_k i \pmod{2^{p-2}} - 2^{p-3}) =$$

$$= \left(\frac{12}{(2^{p-2})} - \frac{24}{(2^{p-2})^3}\right) \sum_{i=0}^{2^{p-2}-1} \left(\frac{i}{2^{p-2}} - \frac{1}{2}\right)\left(\frac{\lambda_k i \pmod{2^{p-2}}}{2^{p-2}} - \frac{1}{2}\right)$$

Так как $\left|\sum_{i=0}^{2^{p-2}-1} \left(\frac{i}{2^{p-2}} - \frac{1}{2}\right)\left(\frac{\lambda_k i \pmod{2^{p-2}}}{2^{p-2}} - \frac{1}{2}\right)\right| \leq \sum_{i=0}^{2^{p-2}-1} \left(\frac{i}{2^{p-2}} - \frac{1}{2}\right)^2 = \frac{2^{p-2}}{12} + \frac{1}{6 \cdot 2^{p-2}},$

то корреляционный коэффициент $\rho^*(X,Y)$ заключен в пределах:

$$\frac{12}{2^{p-2}}\sum_{i=0}^{2^{p-2}-1}\left(\frac{i}{2^{p-2}}-\frac{1}{2}\right)\left(\frac{\lambda_k i(\mathrm{mod}\,2^{p-2})}{2^{p-2}}-\frac{1}{2}\right)-\frac{2}{(2^{p-2})^2}<\rho^*(X,Y)<$$

$$<\frac{12}{2^{p-2}}\sum_{i=0}^{2^{p-2}-1}\left(\frac{i}{2^{p-2}}-\frac{1}{2}\right)\left(\frac{\lambda_k i(\mathrm{mod}\,2^{p-2})}{2^{p-2}}-\frac{1}{2}\right)+\frac{2}{(2^{p-2})^2}.$$

Даже при сравнительно небольших P величиной порядка $2/(2^{p-2})^2$ можно пренебречь, и тогда:

$$\rho^*(X,Y)=\frac{12}{2^{p-2}}\sum_{i=0}^{2^{p-2}-1}\left(\frac{i}{2^{p-2}}-\frac{1}{2}\right)\left(\frac{\lambda_k i(\mathrm{mod}\,2^{p-2})}{2^{p-2}}-\frac{1}{2}\right). \quad (5)$$

Во втором случае, $\lambda\equiv 3(\mathrm{mod}\,8)$, имеем: $\varepsilon_{2i+1}=\varepsilon_1$, $\varepsilon_{2i}=\varepsilon_2$ $(i=0,1,2,\ldots,2^{p-3}-1)$ /15/. Последовательность X распадается на две последовательности, в каждой из них ε_i – постоянная. Тогда мы возвращаемся к предыдущему случаю $\lambda\equiv 5(\mathrm{mod}\,8)$. После аналогичных преобразований получим формулу (5).

В формуле (5) выражение $\frac{\lambda_k i(\mathrm{mod}\,2^{p-2})}{2^{p-2}}$ есть дробная часть $\lambda_k i/2^{p-2}$, обозначаемая обычно $\{\lambda_k i/2^{p-2}\}$.

Подставим $\{\lambda_k i/2^{p-2}\}$ в (5) и преобразуем:

$$\rho^*(X,Y)=\frac{12}{2^{p-2}}\sum_{i=0}^{2^{p-2}-1}\left(\frac{i}{2^{p-2}}-\frac{1}{2}\right)\left(\left\{\frac{\lambda_k i}{2^{p-2}}\right\}-\frac{1}{2}\right)=\frac{12}{(2^{p-2})^2}\sum_{i=0}^{2^{p-2}-1} i\left\{\frac{i\lambda_k}{2^{p-2}}\right\}-3+\frac{6}{2^{p-2}}. \quad (6)$$

Лемма 2.1. Если λ и n – взаимно просты, то $\sum_{i=0}^{n-1}\left[\frac{i\lambda}{n}\right]=\frac{(n-1)(\lambda-1)}{2}$, где $[X]$ – целая часть числа X.

Доказательство:

В силу взаимной простоты λ и n, при каждом i $(0\leqslant i\leqslant n-1)$ величина $\frac{i\lambda}{n}-\left[\frac{i\lambda}{n}\right]=\left\{\frac{i\lambda}{n}\right\}$

принимает различные значения от 0 до $\frac{n-1}{n}$. Тогда: $\sum_{i=0}^{n-1}\left[\frac{i\lambda}{n}\right]=$

$$=\sum_{i=0}^{n-1}\frac{i\lambda}{n}-\sum_{i=0}^{n-1}\left\{\frac{i\lambda}{n}\right\}=\frac{(n-1)\lambda}{2}-\sum_{i=0}^{n-1}\frac{i}{n}=\frac{(n-1)\lambda}{2}-\frac{n-1}{2}=\frac{(n-1)(\lambda-1)}{2},$$

что и требовалось доказать.

Лемма 2.2. Если λ и n – взаимно просты, то $\sum_{i=0}^{n-1}\left\{\frac{i\lambda}{n}\right\}^2=\frac{(n-1)(2n-1)}{6n}$. Доказательство очевидно, если учесть, что при каждом i величина $\left\{\frac{i\lambda}{n}\right\}$ принимает различные значения от 0 до $\frac{n-1}{n}$.

Лемма 2.3. При взаимно простых λ и n:

$$\sum_{i=0}^{n-1}\frac{i}{n}\left\{\frac{i\lambda}{n}\right\}=\frac{\lambda(3n+1)}{12n}+\frac{n-3}{4}+\frac{n^2+1}{12\lambda n}-\sum_{j=0}^{\lambda-1}\frac{j}{\lambda}\left\{\frac{jn}{\lambda}\right\}.$$

Доказательство: При i, изменяющемся от $\left[\frac{(j-1)n}{\lambda}\right]+1$ до $\left[\frac{jn}{\lambda}\right]$ дробная часть $\{i\lambda/n\}$ равна $i\lambda/n-(j-1)$.

Тогда:

$$\sum_{i=0}^{n-1}\frac{i}{n}\left\{\frac{i\lambda}{n}\right\}=\sum_{0}^{\left[\frac{n}{\lambda}\right]}\frac{i^2\lambda}{n^2}+\sum_{\left[\frac{n}{\lambda}\right]+1}^{\left[\frac{2n}{\lambda}\right]}\frac{i}{n}\left(\frac{i\lambda}{n}-1\right)+\ldots+\sum_{\left[\frac{\lambda-2}{\lambda}n\right]+1}^{\left[\frac{\lambda-1}{\lambda}n\right]}\frac{i}{n}\left(\frac{i\lambda}{n}-\lambda+2\right)+$$

$$+\sum_{\left[\frac{\lambda-1}{\lambda}\right]+1}^{n-1}\frac{i}{n}\left(\frac{i\lambda}{n}-\lambda+1\right)=\sum_{i=0}^{n-1}\frac{i^2\lambda}{n^2}+\frac{1}{2n}\sum_{i=0}^{\lambda-1}\left[\frac{in}{\lambda}\right]\left(\left[\frac{in}{\lambda}\right]+1\right)-\frac{(n-1)(\lambda-1)}{2}=$$

$$=\frac{(n-1)(2n-1)\lambda}{6n}+\frac{1}{2n}\sum_{i=0}^{\lambda-1}\left[\frac{in}{\lambda}\right]^2+\frac{1}{2n}\sum_{i=0}^{\lambda-1}\left[\frac{in}{\lambda}\right]-\frac{(n-1)(\lambda-1)}{2}=$$

$$=\frac{(n-1)(2n-1)\lambda}{6n}+\frac{1}{2n}\sum_{i=0}^{\lambda-1}\left(\left\{\frac{in}{\lambda}\right\}^2+\left(\frac{in}{\lambda}\right)^2-2\frac{in}{\lambda}\left\{\frac{in}{\lambda}\right\}+\left[\frac{in}{\lambda}\right]\right)-\frac{(n-1)(\lambda-1)}{2}.$$

Подставим значения вычисленных по лемме 2.1 и лемме 2.2 сумм

$\sum_{0}^{\lambda-1}\left\{\frac{in}{\lambda}\right\}^2$ и $\sum_{0}^{\lambda-1}\left[\frac{in}{\lambda}\right]$, получим:

$$\sum_{i=0}^{n-1}\frac{i}{n}\left\{\frac{i\lambda}{n}\right\} = \frac{(n-1)(2n-1)\lambda}{6n} + \frac{(\lambda-1)(2\lambda-1)}{12n\lambda} + \frac{(\lambda-1)(2\lambda-1)n}{12\lambda} +$$

$$+\frac{(n-1)(\lambda-1)}{4n} - \frac{(n-1)(\lambda-1)}{2} - \sum_{i=0}^{\lambda-1}\frac{i}{\lambda}\left\{\frac{in}{\lambda}\right\} =$$

$$= \frac{(3n+1)\lambda}{12n} + \frac{n-3}{4} + \frac{n^2+1}{12\lambda n} - \sum_{i=0}^{\lambda-1}\frac{i}{\lambda}\left\{\frac{in}{\lambda}\right\}.$$

Лемма доказана.

Обозначим $2^{p-2} = \lambda_0$ и $\lambda = \lambda_1$. λ_0 и λ_1 взаимно просты, поэтому наибольший общий делитель λ_0 и λ_1 равен единице. Рассмотрим известный алгоритм Евклида (доказательство взаимной простоты двух чисел):

$$\begin{aligned}
\lambda_0 &= K_1\lambda_1 + \lambda_2\\
\lambda_1 &= K_2\lambda_2 + \lambda_3\\
\lambda_2 &= K_3\lambda_3 + \lambda_4\\
&\dots\dots\dots\dots\\
\lambda_{s-1} &= K_s\lambda_s + 1\\
\lambda_s &= K_{s+1}\\
\lambda_{s+1} &= 1
\end{aligned} \tag{7}$$

где все числа – целые и положительные, а $K_1, K_2, \dots, K_{s+1}, 1$ – коэффициенты разложения.

Теорема 2.1. Значение корреляционного коэффициента определяется по формуле

$$\rho = \frac{1}{2^{p-2}}\sum_{i=1}^{s+2}(-1)^{i+1}K_i + \varepsilon, \text{ где } |\varepsilon| < 5/2^{p-2}. \tag{8}$$

Доказательство: Преобразуем формулу леммы 2.3, предварительно домножив ее на число 12 :

$$12\sum_{i=1}^{\lambda_0-1}\frac{i}{\lambda_0}\left\{\frac{i\lambda_1}{\lambda_0}\right\} = 3\lambda_1 + \frac{\lambda_1}{\lambda_0} + 3\lambda_0 - 9 +$$

$$+\frac{\lambda_0}{\lambda_1} + \frac{1}{\lambda_0\lambda_1} - \sum_{j=0}^{\lambda_1-1}\frac{j}{\lambda_1}\left\{\frac{j\lambda_0}{\lambda_1}\right\}. \tag{9}$$

Так как из формул (7) следует, что $\left\{\frac{j\lambda_0}{\lambda_1}\right\} = \left\{\frac{j\lambda_2}{\lambda_1}\right\}$, то формула (9) становится рекуррентной: $12\sum_{i=1}^{\lambda_0-1}\frac{i}{\lambda_0}\left\{\frac{i\lambda_1}{\lambda_0}\right\} =$

$$= 3\lambda_1 + \frac{\lambda_0}{\lambda_1} + 3\lambda_0 - 9 + \frac{\lambda_1}{\lambda_0} + \frac{1}{\lambda_0\lambda_1} -$$

$$-3\lambda_2 - \frac{\lambda_1}{\lambda_2} - 3\lambda_1 + 9 - \frac{\lambda_2}{\lambda_1} - \frac{1}{\lambda_1\lambda_2} +$$

$$+3\lambda_3 + \frac{\lambda_2}{\lambda_3} + 3\lambda_2 - 9 + \frac{\lambda_3}{\lambda_2} + \frac{1}{\lambda_2\lambda_3} -$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$+(-1)^s\left(3\lambda_{s+1} + \frac{\lambda_s}{\lambda_{s+1}} + 3\lambda_s - 9 + \frac{\lambda_{s+1}}{\lambda_s} + \frac{1}{\lambda_s\lambda_{s+1}}\right).$$

Отсюда видно, что сумма первых и третьих членов рядов даст $3\lambda_0 + (-1)^s\cdot 3\lambda_{s+1}$, вторых и пятых даст $\sum_{i=1}^{s+1}(-1)^{i+1}K_i + \lambda_1/\lambda_0$, ибо из формул (7) следует: $\lambda_{i-1}/\lambda_i - \lambda_{i+1}/\lambda_i = K_i$, а $\lambda_{s+1} = 1$ и $\lambda_s = K_{s+1}$. Итак,

$$12\sum_{i=1}^{\lambda_0-1}\frac{i}{\lambda_0}\left\{\frac{i\lambda_1}{\lambda_0}\right\} = 3\lambda_0 + \sum_{i=1}^{s+1}(-1)^{i+1}K_i + \frac{\lambda_1}{\lambda_0} + (-1)^s\cdot 3 + \sum_{i=0}^{s}\frac{(-1)^i}{\lambda_i\lambda_{i+1}} - 4{,}5\{1+(-1)^s\}. \tag{10}$$

Сумма знакопеременного ряда $\sum_{i=0}^{s}\frac{(-1)^i}{\lambda_i\lambda_{i+1}}$ не превосходит по абсолютной величине $1/\lambda_s$ и имеет тот-же знак, что и S-тый член суммы. Подставим (10) в выражение корреляционного коэффициента (6): $\rho^*(X,Y)=\rho=\frac{1}{2^{p-2}}\sum_{i=1}^{S+2}(-1)^{i+1}K_i+\mathcal{E}$, где $\mathcal{E}=$

$$=\frac{1}{2^{p-2}}\left\{\frac{\lambda_1}{\lambda_0}+(-1)^s 3+\sum_{i=0}^{s}\frac{(-1)^i}{\lambda_i\lambda_{i+1}}-4{,}5\left[1+(-1)^s\right]+6+(-1)^s\right\}.$$

При S-четном - $\left(1/2^{p-2}<\mathcal{E}<2{,}5/2^{p-2}\right)$, а при S- нечетном - $\left(3{,}5/2^{p-2}<\mathcal{E}<5/2^{p-2}\right)$. Теорема доказана.

Для простоты практического вычисления корреляционного коэффициента введем рекуррентный оператор ν: Пусть дано начальное $\nu_0=\lambda/2^{p-2};\ \nu_{i+1}=1/\{\nu_i\}$.

Тогда формула (8) примет вид:

$$\rho\sim\frac{1}{2^{p-2}}\sum_{0}^{S+1}(-1)^{i+1}[\nu_i]. \tag{11}$$

Вычисление суммы заканчивается, как только ν_i станет целым числом. В формуле (11) отброшены $\mathcal{E}$ и последний член суммы корреляционного коэффициента (8), так как при больших p величинами порядка $5/2^{p-2}$ можно пренебречь.

Возникает вопрос о величине S, имеющей немаловажное значение для практического вычисления. Например, если λ_0 -число Фибоначчи, то алгоритм Евклида (7) будет максимальной длины тогда, когда λ_1 - соседнее меньшее число Фибоначчи. Это видно непосредственно из записи алгоритма Евклида, ибо любое $K_i\neq 1$ сокращает длину алгоритма, а все $K_i=1$ $(i=1,2,\dots,S,S+1)$ при любом S дают числа Фибоначчи. Если λ_0 таково, что лежит между соседними числами Фибоначчи: $F_s<\lambda_0<F_{s+1}$,

то максимальная длина алгоритма Евклида равна S, так как для $\lambda_0=F_s$ длина алгоритма равна S, а для $\lambda_0=F_{s+1}$ равна $S+1$. Итак, если F_s - наибольшее число Фибоначчи, такое, что $F_s<\lambda_0$, то найдется такое $\lambda_1<\lambda_0$, что доказательство взаимной простоты λ_0 и λ_1 потребует максимальное число разложений - S.

Из формулы Бинэ /13/ для общего члена ряда Фибоначчи вычисляется значение S:

$$F_s=\frac{\left(\frac{1+\sqrt5}{2}\right)^s-\left(\frac{1-\sqrt5}{2}\right)^s}{\sqrt5};\quad S\sim\frac{\log_2\lambda_0\sqrt5}{\log_2\frac{1+\sqrt5}{2}}\sim\frac{3}{2}\log_2\lambda_0+2.$$

Если $\lambda_0=2^{p-2}$, то S может достигать величины 1,5 р.

<u>Следствие 2.2.</u> Если найдется такое λ_1, что все K_i $(i=1,2,\dots,S+1)$ равны ℓ, а S нечётно, то при таком λ_1 корреляционный коэффициент ρ достигает локального минимума.

<u>Теорема 2.2.</u> (Обобщенное тождество Симсона).

Если λ_0 и λ_1 таковы, что S нечётно и все $K_i=\ell$, то $\lambda_1^2\,(mod\,\lambda_0)\equiv 1$.

Доказательство: Рассмотрим обобщенный ряд Фибоначчи $F_{n+1}=\ell F_n+F_{n-1}$; $F_0=0$, $F_1=1$. Тождество Симсона для ряда Фибоначчи даётся формулой $f_s^2=f_{s-1}f_{s+1}+(-1)^{s-1}$. Докажем, что оно верно для обобщенного ряда. Формула Бинэ для него даётся в виде

$$F_s=\frac{\left(\frac{\ell+\sqrt{\ell^2+4}}{2}\right)^s-\left(\frac{\ell-\sqrt{\ell^2+4}}{2}\right)^s}{\sqrt{\ell^2+4}}$$

Подстановка F_s в тождество Симсона доказывает справедливость тождества для обобщенного ряда, а справедливость теоремы следует из тождества при S –нечётном, ибо λ_0 и λ_1 – члены обобщенного ряда Фибоначчи.

<u>Следствие 2.3</u>. Если λ_0 и λ_1 – соседние члены обобщенного ряда Фибоначчи, то несмотря на минимальные парные корреляции, датчик с $\lambda = \lambda_1$ следует отвергнуть из-за чрезмерно больших тройных корреляций.

<u>Следствие 2.4</u>. Датчик со значением $\lambda_1 = \lambda \sim \sqrt{\lambda_0}$ должен быть также отвергнут, так как приводит к частному случаю обобщенного ряда Фибоначчи с $l = \lambda_1$ и $S = 1$.

<u>Следствие 2.5</u>. Корреляционный коэффициент находится в пределах $-\frac{1}{3} < \rho < \frac{1}{5}$ для $\lambda \equiv 5 \pmod 8$ и $-1/5 < \rho < 1/3$ для $\lambda \equiv 3 \pmod 8$. Доказательство следует из теоремы 2.1, если придавать λ значения $5,\ 2^{p-2}-3$ и $3,\ 2^{p-2}-5$ соответственно.

<u>Теорема 2.3</u>. Если $\lambda \equiv 2^{p-2} \pm \alpha \pmod{2^{p-2}}$, где $\alpha < \sqrt{2^{p-2}}$, то $|\rho| \sim \frac{1}{\alpha}$.

Доказательство: $\lambda = 2^{p-2} + \alpha \equiv \alpha \pmod{2^{p-2}}$ подставим в формулу (8). Так как $\alpha < \sqrt{2^{p-2}}$, то $K_1 > \sqrt{2^{p-2}}$, а все остальные K_i $(i > 1)$ меньше K_1, то $\rho \sim \frac{K_1}{2^{p-2}} = \frac{1}{2^{p-2}}\left[\frac{2^{p-2}}{\alpha}\right] \sim 1/\alpha$. Для $\lambda = 2^{p-2} - \alpha$, после подстановки в формулу (8) получим: $\rho \sim \left[\frac{2^{p-2}}{2^{p-2}-\alpha}\right] - \left[\frac{2^{p-2}-\alpha}{\alpha}\right] + \ldots \sim \left(1 - \left[\frac{2^{p-2}}{\alpha}\right] + \ldots\right)/2^{p-2}$. Как и в предыдущем случае, все K_i начиная с третьего, меньше K_2, поэтому $\rho \sim -1/\alpha$, что и доказывает теорему.

<u>Теорема 2.4</u>. Если $\lambda = \mu 2^{p-2-t} \pm \alpha$, причём μ – нечётно, $2^{3t}\alpha^2 < 2^{p-2}$, тогда $|\rho| \sim \frac{1}{4^t \alpha}$.

Доказательство: Рассмотрим алгоритм Евклида для чисел 2^t и μ:

$$
\begin{aligned}
2^t = \mu_0 &= k_1\mu_1 + \mu_2 \\
\mu = \mu_1 &= k_2\mu_2 + \mu_3 \\
&\ldots\ldots\ldots \\
\mu_{s-1} &= k_s\mu_s + 1 \\
\mu_s &= k_{s+1} \\
\mu_{s+1} &= 1 \\
\mu_{s+2} &= 0.
\end{aligned}
$$

Тогда, согласно теореме 2.1, $\rho = \frac{1}{2^{p-2}}\{k_1 - k_2 + \ldots \mp k_{s+1}\} \pm \rho(2^{p-2-t} \mp \mu\alpha,\ 2^t\alpha)$. Действительно: $\rho(2^{p-2}, \mu 2^{p-2-t} \pm \alpha) = \rho(2^t \cdot 2^{p-2-t} + 0\cdot\alpha, \mu 2^{p-2-t} \pm 1\cdot\alpha)$, алгоритм Евклида работает до тех пор, пока коэффициенты при 2^{p-2-t} в формуле ρ не станут соответственно 1 и 0, то-есть, коэффициентами при α до работы алгоритма Евклида. По условию, все $k_i < 2^t$, поэтому: $\frac{1}{2^{p-2}}\{k_1 - k_2 + \ldots + k_{s+1}\} < \frac{1}{2^{p-2-t}}$. По теореме 2.3, $\rho(2^{p-2-t} \pm \mu\alpha, 2^t\alpha) \sim \frac{1}{2^{p-2}} \cdot \frac{2^{p-2-t}}{2^t\alpha} = 1/4^t\alpha$, если $\sqrt{2^{p-2-t}} > 2^t\alpha$, то есть, $2^{3t}\alpha^2 < 2^{p-2}$. Так как k_i не могут существенно повлиять на величину ρ (по условию $2^{p-2-t} > 4^t\alpha^2 \geq 4^t\alpha$, так как $\alpha \geq 1$), то теорема доказана.

<u>Следствие 2.6</u>. Значение корреляционного коэффициента $\rho(2^{p-2}, \lambda^{\mu 2^s})$ при больших S $(S > \frac{p}{2} - 3)$ не зависит от λ. Это вытекает из того, что, например, для $\lambda \equiv 5 \pmod 8$, $\lambda^{2^s} \pmod{2^{s+2}} \equiv 1$ и, по теореме 2.4, при $S > \frac{p}{2} - 3$ $|\rho| \sim 1/4^{p-4-s}$ независимо от вида λ.

III. Семейства множителей λ.

Напомним определение группы.

Группой относительно операции $(*)$ называется множество G, в котором выполняются следующие аксиомы:

1. Из $a \in G$, $b \in G$ следует $a * b \in G$.
2. Для любых $a \in G$, $b \in G$, $c \in G$ выполняется $(a * b) * c = a * (b * c)$.
3. Существует единичный $e \in G$ такой, что $e * a = a = a * e$.
4. Для любого $a \in G$ существует обратный элемент a^{-1}, то есть $a * a^{-1} = e$. В работе /15/ выделены четыре вида псевдопоследовательностей, которые может генерировать датчик $x_{n+1} \equiv \lambda x_n (mod\, 2^p)$ в зависимости от вида λ и начального x_0. Последовательности, определяемые

1° $\lambda \equiv 3 (mod\, 8)$, $x_0 \equiv 1 (mod\, 8)$ или $x_0 \equiv 3 (mod\, 8)$

2° $\lambda \equiv 3 (mod\, 8)$, $x_0 \equiv 5 (mod\, 8)$ или $x_0 \equiv 7 (mod\, 8)$

3° $\lambda \equiv 5 (mod\, 8)$, $x_0 \equiv 1 (mod\, 8)$ или $x_0 \equiv 5 (mod\, 8)$

4° $\lambda \equiv 5 (mod\, 8)$, $x_0 \equiv 3 (mod\, 8)$ или $x_0 \equiv 7 (mod\, 8)$

образуют четыре вида конечных циклических групп с циклическим порождающим λ.

Последовательности 1° и 3° являются группами относительно операции умножения по $mod\, 2^p$: $(x \in G,\ y \in G,\ xy (mod\, 2^p) \in G)$, а последовательности 2° и 4° – относительно операции умножения с дополнительным умножением на константу семь по $mod\, 2^p$: $(x \in G,\ y \in G,\ x * y = 7xy (mod\, 2^p) \in G)$.

Единичные элементы равны: для 1° и 3° обычной единице, а для 2° и 4° (запись в двоичной системе счисления):

$$10110110110 \ldots 110110110111 (mod\, 2^p) \equiv 7^{-1} (mod\, 2^p)$$

Так как датчик (1) имеет более общую запись (12):

$x_n \equiv \lambda^n x_0 (mod\, 2^p)$, то непосредственная проверка $1^\circ - 4^\circ$ убеждает в справедливости для последовательностей аксиом 1-4.

Из теории циклических групп хорошо известно, что если K взаимно просто с 2^p, то есть, нечётно, то $\lambda^K (mod\, 2^p)$ будет порождающим элементом той же группы. Так $\lambda \equiv 3 (mod\, 8)$ в любой нечётной степени будет порождающим для 1° и 2°, а $\lambda \equiv 5 (mod\, 8)$ - для 3° и 4°. Этот факт используется в данной работе.

Так как период датчика (12) равен 2^{p-2}, то есть /4/: $\lambda^{2^{p-2}} (mod\, 2^p) \equiv 1$, то $\lambda^{2^{p-2}+K} \equiv \lambda^K (mod\, 2^p)$, поэтому степени λ будут рассматриваться по $mod\, 2^{p-2}$.

<u>Определение 3.1</u>. λ_1 и λ_2 принадлежат одному семейству, если найдутся целые постоянные n и R, для которых справедливо одно из двух сравнений: $x_i^1 \equiv x_{i+n}^2 + R (mod\, 2^p)$,

$x_i^1 \equiv x_{n-i}^2 + R (mod\, 2^p)$, $(i = 1, 2, \ldots, 2^{p-2})$,

где x_i^1 и x_i^2 - члены псевдопоследовательностей, генерированных датчиками с λ_1 и λ_2 соответственно.

<u>Определение 3.2</u>. Если $\lambda \equiv 5^\tau (mod\, 2^p)$ или $\lambda \equiv 3^\tau (mod\, 2^p)$, то такое λ является членом τ-семейства.

<u>Теорема 3.1</u>. Множители $\lambda(\tau, K) \equiv 5^{(K \cdot 2^{p-4} \pm \tau)(mod\, 2^{p-2})} (mod\, 2^p)$, где τ - нечётно, а $K = 1, 2, 3, 4$ образуют τ - семейство, состоящее из восьми различных множителей.

Множители $\lambda(\tau,K)\equiv 3^{(K\cdot 2^{p-3}\pm\tau)(mod\, 2^{p-2})}(mod\, 2^p)$, где τ -нечётно, а $K=1,2$ образуют τ-семейство, состоящее из четырех различных множителей.

Доказательство проведем для первого случая, так как для второго доказывается аналогично. Пусть $\lambda\equiv 5^{\tau}(mod\, 2^p)$. Покажем, что найдутся R, t, n, что $5^{\tau i}(mod\, 2^p)+$ $+R\equiv(5^{\tau+t\cdot 2^{p-5}})^{i+n}(mod\, 2^p)$. Здесь знаки τ в правой и левой частях сравнения совпадают; при несовпадении вместо $i+n$ в правой части нужно поставить $n-i$. $t=1,2,\dots,7$. Так как $5=1+2^2$, то преобразуем сравнение, возведя в степень: $5^{\tau i(mod\, 2^{p-2})}(mod\, 2^p)+R\equiv$

$$\equiv 5^{(\tau i+ti2^{p-5}+\tau n+tn2^{p-5})(mod\, 2^{p-2})}(mod\, 2^p)\equiv$$

$$\equiv 5^{\tau i}[1+2^{p-3}ti+2^{p-2}(ti2^{p-5}-1)+\dots][1+2^2\tau n+2^3\tau n(\tau n-1)+\dots]$$

$$[1+tn2^{p-3}+\dots](mod\, 2^p)\equiv 5^{\tau i}[1+2^2\tau n+2^3\tau n(\tau n-1)+\dots+$$

$$+2^{p-3}ti+2^{p-2}ti(ti2^{p-5}-1)+\dots][1+tn2^{p-3}+\dots](mod\, 2^p).$$

Поскольку n - чётное, имеем:

$$R\equiv 5^{\tau i}[2^2\tau n+2^3\tau n(\tau n-1)+\dots$$

$$+2^{p-3}ti+2^{p-2}ti(ti2^{p-5}-1)+\dots](mod\, 2^p)\equiv$$

$$\equiv[1+2^2\tau i+2^3\tau i(\tau i-1)+\dots][2^2\tau n+2^3\tau n(\tau n-1)+\dots+$$

$$+2^{p-3}ti+2^{p-2}ti(ti2^{p-5}-1)+\dots](mod\, 2^p)\equiv\{[2^2\tau n+2^3\tau n(\tau n-1)+\dots]+$$

$$+2^4 i[\tau^2 n+2\tau^2 n(\tau n-1)+\dots+2\tau^2 n(\tau i-1)+2^2\tau^2 n(\tau n-1)(\tau i-1)+\dots+$$

$$+2^{p-7}t(ti2^{p-5}-1)+\dots+2^{p-5}t\tau i(ti2^{p-5}-1)+\dots]\}(mod\, 2^p).$$

На определение чисел n и t в этом сравнении не влияют члены, не зависящие от i. Для того, чтобы сравнение было тождественно равно константе R, нужно, чтобы при различных i сумма членов, зависящих от i была равна нулю. Положив $n=$ $=s\cdot 2^{p-7}$, s - нечётно покажем, что даже при этом n со сравнительно большой степенью двойки, это невозможно:

$$2^4 i[\tau^2 s\cdot 2^{p-7}+2^{p-6}\tau^2 s(2^{p-7}-1)+\dots+2^{p-6}\tau^2 s(\tau i-1)+$$

$$+2^{p-5}\tau^2 s(2^{p-7}-1)(\tau i-1)+\dots+2^{p-7}t(2^{p-5}-1)+\dots+2^{p-5}\tau ti(2^{p-5}-1)+\dots]$$

$$(mod\, 2^p)\equiv 2^4 i[2^{p-7}\tau^2 s(2^{p-7}-1)+\dots+2^{p-6}\tau^2 s(\tau i-1)(2^{p-7}-1)+\dots$$

$$+2^{p-7}t(2^{p-5}-1)+\dots+2^{p-5}\tau ti(2^{p-5}-1)+\dots](mod\, 2^p) \qquad (13)$$

Если t - чётно, то все члены суммы (13) равны нулю по $mod\, 2^{p-2}$, за исключением первого, который будет зависеть от i и равен нулю по $mod\, 2^{p-2}$ тогда, когда $i\equiv$ $\equiv 0\,(mod\, 2)$. Если t нечётно, тогда сравнение (13) преобразуется к виду: $i[S_1 + 3S(\tau i-1) + 2i](mod 4)$ где $S_1 \equiv (7S + 7t)/2 \ (mod 4)$. Отсюда видно, что при $i = 1$ постоянная S_1 должна быть чётной, а при $i = 2$ – нечётной, чтобы выполнялось $i[S_1 + 3S(\tau i-1) + 2i](mod 4) \equiv 0$. Полученное противоречие доказывает невозможность $n = S \cdot 2^{p-7}$. Аналогично покажем, что при $n = S \cdot 2^{p-6}$, S – нечётно, найдется такое t, что сравнение (13) тождественно равно нулю: $i[6S_1 + 6S(\tau i-1) + 7t + 4ti](mod 8)$. Отсюда видно, что t чётно, и $i[S_1 + 2(\tau i-1)](mod 4) \equiv 0$ в том случае, если $S_1 \equiv 0 \ (mod 4)$. Так как $S_1 \equiv 0 \ (mod 8) \equiv 6S + 6t_1 (mod 8)$, где $2t_1 = t$, S – нечётно, то t_1 – также нечётно. Подставив $t = 2t_1$ в исходную формулу, заметим, что $t_1 = K$ в формулировке теоремы. Теорема доказана.

Следствие 3.1. Если $\lambda (mod 2^p)$ принадлежит τ-семейству, то $(\lambda + K_1 \cdot 2^{p-2})(mod 2^p)$ и $(\lambda^{-1} + K_2 \cdot 2^{p-2})(mod 2^p)$, где K_1 и K_2 – целые, также принадлежат τ - семейству. Из доказательства теоремы 3.1, как следствие, имеем:

Теорему 3.2. τ - семейство состоит только из множе[redacted] вида $5^{(K \cdot 2^{p-4} \pm \tau)(mod 2^{p-2})} (mod 2^p)$ и $3^{(K \cdot 2^{p-3} \pm \tau)(mod 2^{p-2})} (mod 2^p)$, то есть не существует множителей λ, входящих в τ - семейство и имеющих иное представление.

В главе второй упоминается об обратном множителе для λ, таком, что $\lambda \lambda^{-1} \equiv 1 \ (mod 2^p)$. Согласно определению группы, тот элемент является единственным для каждого λ. Так

как $\lambda^{2^{p-2}} (mod 2^p) \equiv 1$, и, представив λ в виде $5^\tau \ (mod 2^p)$, либо $3^\tau (mod 2^p)$, получим:

Лемма 3.1. Для $\lambda \equiv 5^\tau (mod 2^p)$ и $\lambda \equiv 3^\tau (mod 2^p)$ обратными будут $\lambda^{-1} \equiv 5^{2^{p-2}-\tau} (mod 2^p)$ и $\lambda^{-1} \equiv 3^{2^{p-2}-\tau} (mod 2^p)$ соответственно.

Лемма 3.2. Для любого a, $a^{-1}(mod 8) \equiv a$. Доказывается непосредственной проверкой.

Лемма 3.3. Обратный множитель λ^{-1} будет генерировать обратную последовательность (по отношению к последовательности с множителем λ), то есть, найдется такое n, что $x_i = x_{n-i}^{-1}$ для всех i, в том случае, если x_0^{-1} принадлежит группе с порождающим λ.

Действительно, в этом случае λ и λ^{-1} будут порождающими элементами одной и той же группы. Умножив левую и правую часть сравнения $x_{i+1} \equiv \lambda x_i (mod 2^p)$ на λ^{-1} получим искомое.

Теорема 3.3. Число семейств для $\lambda \equiv 5 \ (mod 8)$ равно 2^{p-6}, а для $\lambda \equiv 3 (mod 8)$ равно 2^{p-5}. Семейство однозначно характеризуется целым нечётным числом $1 \leq \tau \leq 2^{p-5} - 1$ для первого случая, и целым нечётным числом $1 \leq \tau \leq 2^{p-4} - 1$ – для второго.

На самом деле, τ – минимальная степень, в которую надо возвести пять или три, чтобы полученное λ, согласно теореме 3.1, принадлежало τ-семейству. Однозначность следует из теоремы 3.2.

Смысл введенного понятия семейства проясняется, если на окружности равномерно и последовательно нанести все числа последовательности и соединять соответствующие точки окружности по мере образования новых x_i (см.рис.). В результате получим замкнутую ломаную. Для множителей λ, принадлежащих одному семейству, вращением чертежа вокруг центра ломаные можно совместить, что не удаётся для λ, принадлежащих разным семействам. Чертежи для λ и λ^{-1} совпадают. Предполагается, что во всех случаях x_0 одно и то же. На рисунке три чертежа: $\lambda \equiv 5$; $\lambda \equiv 13$; $\lambda \equiv 21 \pmod{2^8}$. $x_0 = 1$. $\lambda = 5$ и $\lambda = 13$ принадлежат одному семейству, а $\lambda = 21$ – другому.

Итак, каждому λ соответствует некоторое нечётное число τ, называемое номером семейства. Из исходной формулы вывода корреляционного коэффициента (4) получаем:

Лемму 3.4. Корреляционный коэффициент $\rho(\lambda) = \rho(\lambda^{-1})$.

Доказательство следует из того, что $x_{i+1} \equiv \lambda x_i \pmod{2^p}$ равносильно $\lambda^{-1} x_{i+1} \equiv x_i \pmod{2^p}$.

Согласно следствию 2.5, максимальные корреляции будут иметь последовательности, генерированные $\lambda = 3$, $\lambda = 5$, $\lambda = 2^p - 3$, $\lambda = 2^p - 5$. Задача выбора множителя λ, дающего наилучшую в статистическом смысле псевдопоследовательность сводится к нахождению такого τ-семейства, то есть такого числа τ ($\lambda \equiv 5^\tau \pmod{2^p}$ или $\lambda \equiv 3^\tau \pmod{2^p}$), чтобы при возможно большем m, $\lambda_m \equiv 5^{\tau m} \pmod{2^p} \equiv 5^{\tau^\circ} \pmod{2^p}$ или $\lambda_m \equiv 3^{\tau m} \pmod{2^p} \equiv 3^{\tau^\circ} \pmod{2^p}$ мы попадали в τ°-семейство (определяемое по теореме 3.1), характеризуемое неудовлетворительными статистическими свойствами. Если, например, корреляционный коэффициент τ°-семейства слишком велик, мы должны τ выбирать таким образом, чтобы в выражении $\tau m \pmod{2^{p-4}} \equiv \tau^\circ$, m достигало максимума.

Используя теоремы 2.3 и 2.4 можно определить такие λ (а, следовательно, и семейства), корреляционный коэффициент которых не превосходит заданного числа.

Определение 3.3. Если корреляционный коэффициент множителя λ, взятый по абсолютной величине, не превосходит числа $\ell/100$, то будем говорить, что λ обладает $\ell\%$-уровнем или просто ℓ-уровнем.

Теоремы 2.3 и 2.4 позволяют найти некоторые λ, не соответствующие ℓ-уровню, но не все. Для того, чтобы найти все такие множители λ, воспользуемся обобщением теоремы 2.4:

Теорема 3.4. Если числа a и b взаимно просты, $a < b$ и найдется такое α (необязательно целое), что $\lambda = \frac{a}{b} \cdot 2^{p-2} \pm \alpha$, причём $b^3 \alpha^2 < 2^{p-2}$ и $b^3 \alpha < 2^{p-2}$, тогда $|\rho| \sim 1/b^2\alpha$.

Доказательство проводится аналогично доказательству теоремы 2.4, если учесть, что α может быть меньше единицы, и условие $b^3 \alpha < 2^{p-2}$, опущенное в доказательстве теоремы 2.4, здесь не является лишним.

Если корреляционный коэффициент некоторого λ не соответствует ℓ уровню ($\ell/100 > 1/\sqrt{2^{p-2}}$), то в выражении (8) найдется такой коэффициент K_i, больший всех остальных, что $K_i/2^{p-2} > \ell/100$. Этот K_i будет определять величину и знак корреляционного коэффициента. Рассмотрим числа $K_1, K_2, \ldots, K_{i-1}$. Можно рассматривать и числа K_{i+1}, $K_{i+2}, \ldots, K_{s+1}$, так как по лемме 3.4 корреляционные коэффициенты $\rho(\lambda)$ и $\rho(\lambda^{-1})$ равны, а выражение (8) для $\rho(\lambda^{-1})$ будет отличаться от $\rho(\lambda)$ обратным порядком чисел K_i.

Если $i=1$, то все λ, не соответствующие ℓ-уровню находятся по теореме 2.3. Если $i=2$, то $K_2 = K$ и $\lambda_j = 2^{p-2}/K_1 - \alpha(K_1) - 8j$, где $0 < \alpha(K_1) < 8$, таково, что $\lambda_j \equiv 5 \pmod 8$, а $j = 0,1,2,\dots$, для которых $\ell/100 < 1/K_1^2[\alpha(K_1)+8j]$ (в соответствии с теоремой 3.4). Присваивая K_1 значения $1, 2, \dots$ найдем все множители λ для $i=2$. Аналогично, для $i=3$, $K_3 = K$ и $\lambda_j = \frac{2^{p-2}K_1}{K_1K_2+1} + \alpha(K_1K_2) + 8j$. Находятся все λ_j, для которых $\ell/100 < 1/(K_1K_2+1)^2[\alpha(K_1K_2)+8j]$. Для $i=4$ $\lambda_j = \frac{2^{p-2}(K_1K_2+1)}{K_1K_2K_3+K_1+K_3} - \alpha(K_1K_2K_3) - 8j$ и т.д. Таким образом находятся все множители λ, не соответствующие ℓ-уровню, так как описанный алгоритм – полный перебор алгоритмов Евклида для чисел 2^{p-2}, λ, где $\lambda \equiv 5 \pmod 8$ и разложение (7) имеет коэффициент $K_i(\lambda) > 2^{p-2}\ell/100$. Разумеется, среди всех выбранных λ найдутся обратные друг другу. Исключая по одному из таких пар, получаем набор множителей, определяющих все семейства, не соответствующие ℓ-уровню.

Пусть выбраны все λ, корреляционный коэффициент которых превосходит ℓ-ровень, (по теореме 2.3, 2.4 и 3.4): $\lambda_0, \lambda_1, \dots, \lambda_q$, и найдены семейства (номера семейств), которым принадлежат эти множители: $\{\tau_0, \tau_1, \dots, \tau_q\} = R$

Из теорем 3.1 и 3.3 следует:

Определение 3.4. Если $\lambda \equiv 5^t \pmod{2^p}$, то семейство (номер семейства) τ определяется формулой:

$$\tau = \min\{t \pmod{2^{p-4}}, (2^{p-4}-t) \pmod{2^{p-4}}\}$$

и, аналогично, если $\lambda \equiv 3^t \pmod{2^p}$, то

$$\tau = \min\{t \pmod{2^{p-3}}, (2^{p-3}-t) \pmod{2^{p-3}}\},$$

где t – нечётно.

Эту операцию будем обозначать $\tau(t)$. Пусть в дальнейшем $\tau_0 = 1$, то есть τ_0 – первое семейство, которому принадлежат, в част ности, 5 и 3.

Определение 3.5. Семейство L называется ℓ-оптимальным, если $L \notin R$, $\tau(3L) \notin R$, $\tau(5L) \notin R, \dots, \tau[(m-2)L] \notin R$, $\tau(mL) \notin R$, $\tau[(m+2)L] \in R$ и нечётное число $m(L)$ достигает максимума. Множители λ, принадлежащие семейству L, будем называть ℓ-оптимальными, а число m – ℓ-оптимальной характеристикой. Это число – максимальная длина последовательности, никакие пары членов которой не имеют корреляционного коэффициента, превышающего ℓ-уровень.

Теорема 3.5. (получение ℓ-характеристики произвольного λ). Если $\lambda \equiv 5^T \pmod{2^p}$ или $\lambda \equiv 3^T \pmod{2^p}$, то ℓ-характеристика λ равна

$$m = \min\{\tau(T^{-1}), \tau(\tau_1 \cdot \tau(T^{-1})), \dots, \tau(\tau_q \cdot \tau(T^{-1}))\}$$

Для доказательства выпишем цепочку равенств:

$$\tau(\tau(T) \cdot m_0) = \tau_0 = 1$$

$$\tau(\tau(T) \cdot m_1) = \tau_1$$

. . . .

$$\tau(\tau(T) \cdot m_q) = \tau_q$$

Здесь m_i - некоторые нечётные числа. Нас должны интересовать m_i, которые находятся согласно определению 3.4:

$$m_0 = \tau(T^{-1})$$

$$m_1 = \tau(\tau_1\cdot\tau(T^{-1}))$$

. . . .

$$m_q = \tau(\tau_q\cdot\tau(T^{-1}))$$

m_i - наименьшая степень, в которую надо возвести множитель $\lambda\equiv 5^T(\mathrm{mod}\,2^p)$ или $3^T(\mathrm{mod}\,2^p)$ чтобы полученное после возведения в степень λ^{m_i} принадлежало семейству τ_i. Минимальное из m_i даст нам m, то-есть ℓ-характеристику λ.

Следствие 3.2. ℓ - характеристика, при любом ℓ, не превосходит $2^{p-5}-1$ для $\lambda\equiv5(\mathrm{mod}\,8)$ и $2^{p-4}-1$ для $\lambda\equiv3(\mathrm{mod}\,8)$. Следствие даёт верхнюю границу для определения объёма псевдопоследовательности.

Теорема 3.6 (получение ℓ-оптимального семейства и ℓ-оптимальной характеристики).

1. ℓ - оптимальная характеристика.

$$m = \max_j\{\min_i[2^{p-5}-2j+1,\ \tau(\tau_i\cdot(2^{p-5}-2j+1))]\}$$

где

$$i = 1,2,\dots,q;\quad j=1,2,3,\dots$$

2. Номер ℓ-оптимального семейства равен $N = \tau[(2^{p-5}-2j+1)^{-1}]$.

3. Одно из семейства ℓ-оптимальных множителей $\lambda\equiv 5^{\tau[(2^{p-5}-2j+1)^{-1}]}(\mathrm{mod}\,2^p)$. Теорема приведена для случая $\lambda\equiv5\,(\mathrm{mod}\,8)$. Изменения для случая $\lambda\equiv3\,(\mathrm{mod}\,8)$ ясны из теорем 3.1, 3.2, 3.3.

Теорема - запись алгоритма для нахождения ℓ-оптимальной характеристики и ℓ-оптимального семейства. Напервом шаге проверяется максимально возможное число (согласно следствию 3.2) $2^{p-5}-1$, затем меньшее соседнее $2^{p-5}-3$ и т.д. Наибольшая из получающихся характеристик и будет ℓ-оптимальной. Алгоритм прекращает свою работу, как только при некотором j величина $2^{p-5}-2j+1$ станет меньше или равна $\min_i\tau(\tau_i\cdot(2^{p-5}-2j+1)),\ i=1\div q$, ибо все остальные характерьстики будут меньше $2^{p-5}-2j+1$.

IУ. Псевдослучайное число как логическая шкала.

Псевдопоследовательности,. генерируемые мультипликативным датчиком, обладают следующим недостатком. Если нужен случайный двоичный набор (логическая шкала), то, как показано в /14, 15/ младшие разряды псевдослучайного числа по сравнению с более старшими все хуже удовлетворяют критериям случайности, а последние (самые младшие) даже вырождаются в постоянные (0 или 1). Так, для $\lambda\equiv5\,(\mathrm{mod}\,8)$ последний и предпоследний разряды всегда равны 01 (если $x_0\equiv1\,(\mathrm{mod}\,4)$), а для $\lambda\equiv3\,(\mathrm{mod}\,8)$ последний и третий от конца разряды равны $0\varepsilon1$ (если $x_0\equiv1;3\,(\mathrm{mod}\,8)$).

Для устранения этого недостатка предлагается следующая модернизация датчика, легко осуществляемая на ЭВМ некоторых типов. Пусть дан датчик $x_{i+1}\equiv\lambda x_i\ (\mathrm{mod}\,2^p)$. На его основе будем получать новое псевдослучайное число - логическую шкалу y_{i+1}:

$$y_{i+1}\equiv\left(x_{i+1}+\left[\frac{x_i\lambda}{2^p}\right]\right)(\mathrm{mod}\,2^p)\equiv\left(x_i\lambda+\left[\frac{x_i\lambda}{2^p}\right]\right)(\mathrm{mod}\,2^p) \qquad (14)$$

Целая часть $\left[\frac{x_i\lambda}{2^p}\right]$ – старшие разряды произведения $x_i\lambda$, не используемые при обычной работе датчика.

Преобразование базируется на том широко известном факте, что если α –случайное число, равномернораспределенное в интервале /0,1/, то $(\alpha+C)(mod\,1)$ будет также случайным числом, равномернораспределенным в /0,1/ независимо от вида константы C. Рассмотрим последние S разрядов псевдослучайного числа y_{i+1}. Период последовательности чисел, являющихся S последними разрядами чисел x_i исходного датчика, равен 2^{S-2}. Последние S разрядов числа $[x_i\lambda/2^p]$ – это средние разряды произведения $x_i\lambda$, то-есть разряды, наиболее полно отвечающие критериям случайности, а если S не слишком велико, то с некоторым допущением можно говорить о последних разрядах числа $[x_i\lambda/2^p]$ как о первых (старших) разрядах псевдослучайного числа $x_i\lambda(mod\,2^{p+s})$. Поэтому, предполагая последние S разрядов числа $[x_i\lambda/2^p]$ случайными, можно рассматривать последовательность Y как сумму последовательностей:

$$y_{K\cdot 2^{s-2}+1} \equiv \left(x_{K\cdot 2^{s-2}}\lambda + \left[\frac{x_{K\cdot 2^{s-2}}\lambda}{2^p}\right]\right)(mod\,2^p)$$

$$y_{K\cdot 2^{s-2}+2} \equiv \left(x_{K\cdot 2^{s-2}+1}\lambda + \left[\frac{x_{K\cdot 2^{s-2}+1}\lambda}{2^p}\right]\right)(mod\,2^p)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y_{(K+1)2^{s-2}} \equiv \left(x_{(K+1)2^{s-2}-1}\lambda + \left[\frac{x_{(K+1)2^{s-2}-1}\lambda}{2^p}\right]\right)(mod\,2^p)$$

При $K=0,1,\ldots$ для каждой из последовательностей последние S разрядов числа $y_{K\cdot 2^{s-2}+j}$ представляются суммой предполагаемого случайного числа $[x_i\lambda/2^p](mod\,2^s)$ и константы. Статистические качества этих S разрядов определяются, очевидно, только S последними разрядами $[x_i\lambda/2^p]$. С другой стороны, старшие (первые) разряды логической шкалы y_{i+1} будут, в основном определяться старшими разрядами числа $x_i\lambda(mod\,2^p)$. На ЭВМ типа М-20 к датчику добавляется одна команда типа сложения /14/:

$æ+0$	065	$\langle x_0\rangle$	$\langle\lambda\rangle$	σ	умножение
1	047	0000	0000	$\langle x_0\rangle$	выдача мл. разрядов
2	013	$\langle x_0\rangle$	σ	$\langle y\rangle$	сложение

(15)

В рабочей ячейке σ получается величина $[x_i\lambda/2^{36}]$, а в ячейке $\langle y\rangle$ – логическая шкала $y_{i+1}\equiv(x_i\lambda + [x_i\lambda/2^{36}])(mod\,2^{36})$. Так как вид псевдослучайного числа, как логической шкалы, не отличается от вида первоначального псевдослучайного числа x_{i+1} (например, порядок в обоих случаях нулевой – число ненормализованное), то вполне возможно употребление датчика (15) не только как логического набора, но и как обычного, числового генератора псевдослучайных чисел, равномернораспределенных в /0,1/ тем более, что его статистические качества ожидаются более высокими, нежели исходного.

Итак, можно рекомендовать датчик $y_{i+1}\equiv(x_i\lambda + [x_i\lambda/2^p])(mod\,2^p)$ как универсальный, то есть, пригодный для логических и числовых вычислений.

У. Алгоритмы и программы.

5.1. Вычисление корреляционного коэффициента.

Из теоремы 2.1 и формулы (11) следует способ вычисления корреляционного коэффициента для любого λ. Находя значения коэффициента для $\lambda^1, \lambda^2 (mod\, 2^{p-2}), \ldots$ мы получаем численное выражение зависимости между соседними членами псевдопоследовательности $(\rho(2^{p-2}, \lambda^1))$, первым и третьим $(\rho(2^{p-2}, \lambda^2 (mod\, 2^{p-2})))$ и т.д. Если требуется последовательность из L псевдослучайных чисел, то нужно найти все значения корреляционного коэффициента $\rho(2^{p-2}, \lambda^K (mod\, 2^{p-2}))$, где $K = 1, 2, 3, \ldots, L$. Если все значения коэффициента меньше по абсолютной величине некоторого ε $(0 < \varepsilon < 1/3)$, то выбранное λ считаем подходящим для вычислений.

Запишем алгоритм вычисления корреляционного коэффициента по шагам:

1° Положим $i = 0$.

2° Вычислим $\nu_0 = 2^{p-2} / \lambda^K (mod\, 2^{p-2})$

3° $\rho'_K = [\nu_0]$

4° $\nu_{i+1} = 1/\{\nu_i\}$, $\rho'_K = \rho'_K + (-1)^{i+1} [\nu_{i+1}]$

5° Если $\nu_{i+1} \neq [\nu_{i+1}]$, переходим к шагу 6°, иначе 7°.

6° Положим $i = i + 1$ и перейдем к 4°.

7° Положим $\rho_K = \rho'_K / 2^{p-2}$

8° Конец работы алгоритма.

Интервал $/0, 1/3/$ разбиваем на отрезки: $(1/2^3, 1/3), (1/2^5, 1/2^3), (1/2^7, 1/2^5), \ldots$ Запоминается количество абсолютных значений корреляционного коэффициента, попавших в данный отрезок. Запоминается количество абсолютных значений корреляционного коэффициента, попавших в данный отрезок. Запоминается также наименьший номер K_i (показатель степени λ), при котором произошло попадание в j-тый отрезок. Полученный спектр значений корреляционного коэффициента характеризует последовательность, генерированную множителем λ.

Данная программа, как и все последующие составлены для ЭВМ "Минск-22". Время счёта для $L = 2^{18} \sim 250\,000$ около 3,5 часов.

5.2. Вычисление λ^{-1}.

а) Рассмотрим два алгоритма для вычисления λ^{-1}. При вычислении по первому способу находим такое S, что $5^S \equiv$ $\equiv \lambda (mod\, 2^p)$, тогда $\lambda^{-1} \equiv 5^{2^{p-2} - S} (mod\, 2^p)$ (по лемме 3.1). Даны $\lambda = \varepsilon_p, \varepsilon_{p-1}, \ldots, \varepsilon_1$ - двоичное представление λ; массив степеней $5^{2^i} (mod\, 2^p)$ $(i = 0, 1, \ldots, p-3)$

Обозначим $e_i = \underbrace{00\ldots0}_{p-i}1\underbrace{0\ldots0}_{i-1}$

Рассмотрим алгоритм по шагам:

1° Положим $S = 0$, $\lambda^* = e_3$, $j = 0$.

2° Если $\lambda \wedge e_{j+3} = \lambda^* \wedge e_{j+3}$, перейдем к 3°, иначе $\lambda^* = \lambda^* \cdot 5^{2^j}$, $S = S + 2^j$

3° Если $j = p - 3$, то 4°, иначе $j = j + 1$ и перейдем к 2°.

4° Вычислим $S' = (2^{p-2} - S) (mod\, 2^{p-2})$ и $\lambda^{-1} \equiv$ $\equiv 5^{S'} (mod\, 2^p)$

5° Конец работы алгоритма.

б) Прямое получение λ^{-1}. Пусть $\lambda^{-1} = 1 + 2^{i_1} + 2^{i_2} + \ldots + 2^{i_s}$.

Так как $\lambda \lambda^{-1} \equiv 1 (mod\, 2^p)$, то $1 \equiv (\lambda + 2^{i_1}\lambda + 2^{i_2}\lambda + \ldots$ $+ 2^{i_s}\lambda) (mod\, 2^p)$. Тогда $1 - \lambda \equiv (2^{i_1}\lambda + 2^{i_2}\lambda + \ldots$ $+ 2^{i_s}\lambda) (mod\, 2^p)$ и на i_1-м месте в двоичном разложении числа $(1-\lambda)(mod\, 2^p)$ стоит первая (младшая) единица. Поскольку i_1 найдено, получим: $1-\lambda-2^{i_1}\lambda \equiv (2^{i_2}\lambda + \dots + 2^{i_s}\lambda)(mod\, 2^p)$. Отсюда находим i_2 и т.д.

Дано λ. Запишем алгоритм вычисления λ^{-1}.

1°. Положим $f = e_1$, $\lambda^{-1} = 0$, $j = 1$

2°. Если $f \wedge e_j \neq \lambda \cdot e_j$, перейдем к 3°, иначе $\lambda^{-1} = \lambda^{-1} \oplus e_j$, $f = (f-\lambda)(mod\, 2^p)$, $\lambda = 2\lambda(mod\, 2^p)$.

3°. Если $j = p$, перейдем к 4°, иначе $j = j+1$ и перейдем к 2°.

4°. Конец работы алгоритма.

Здесь $\oplus$ означает поразрядное сложение. Этот алгоритм используется в программах, так как является более экономным и быстрым, чем первый.

5.3. Получение степеней.

Для оценки λ (по теореме 3.5) необходимо найти ряд степеней, соответствующих выбранным λ_i. λ_i находятся согласно теоремам 3.4, 2.3 и 2.4. Например, если $\ell = 1$, то таких степеней нужно найти 45 (число семейств, превосходящих ℓ-уровень); если $\ell = 0{,}1$, то число семейств, а, следовательно, и множителей λ_i, для которых нужно находить их степени, равно 610.

Для этой цели подходит алгоритм 5.2 а).

Найдены все степени пятерки, отвечающие $\ell = 0{,}1$. В их число, естественно, входят и 45 степеней, отвечающих $\ell = 1$.

5.4. Вычисление ℓ-характеристики λ.

Возможны два варианта представления λ при определении его ℓ-характеристики:

1. $\lambda \equiv 5^T(mod\, 2^p)$ (то есть дано T).

2. $\lambda \equiv 5\,(mod\, 8)$ (дано λ – восьмеричное число).

Для двух вариантов составлены программы получения ℓ-характеристик сразу для некоторого набора множителей λ. Алгоритм задаётся теоремой 3.5. Время работы алгоритма – мало: для 100 множителей характеристики подсчитываются менее минуты.

5.5. Получение ℓ-оптимальной характеристики и семейства.

Теорема 3.6 даёт алгоритм нахождения ℓ-оптимальной характеристики и ℓ-оптимального семейства.

Результат работы программы – те семейства и их характеристики, которые больше всех предыдущих, то есть программа фиксирует приближение к ℓ-оптимальному семейству.

Все программы составлены для случая $\lambda \equiv 5\,(mod\, 8)$, однако переход к $\lambda \equiv 3\,(mod\, 8)$ несложен.

У1. Результаты и выводы

Для $\lambda = 5^{2i+1} (\mathrm{mod}\, 2^{36})$ были найдены 0,1 - характеристики $(i = 0, 1, 2, \ldots, 99)$, то есть длины последовательностей, для которых корреляционный коэффициент меньше 1/1000. В таблице 1 первое число - $2i + 1$, второе - 0,1 характеристика

1 - 1	41-6,7.10^5	81-2,6.10^5	121-6,3.10^6	161-1,6.10^6
3 - 1	43-3,4.10^6	83-3.10^6	123-5,1.10^6	163-1,9.10^6
5-3,5.10^5	45-5.10^5	85-2.10^4	125-1,4.10^6	165-4.10^6
7-7.10^6	47-10^6	87-2,5.10^5	127-2,5.10^6	167-5.10^6
9-2,4.10^6	49-3,5.10^6	89-1,2.10^6	129-5,6.10^6	169-3,8.10^6
11-3,4.10^6	51-2.10^7	91-4,1.10^6	131-1,3.10^4	171-5.10^5
13-2,8.10^6	53-2,5.10^6	93-1,9.10^6	133-6,3.10^5	173-4,5.10^6
15-1,4.10^6	55-3,3.10^6	95-9,6.10^6	135-1,6.10^5	175-10^6
17-10^5	57-1,5.10^6	97-5.10^6	137-2,3.10^6	177-1,2.10^6
19-1,4.10^6	59-9,1-10^5	99-9.10^5	139-3,4.10^6	179-907
21-4.10^6	61-9.10^5	101-3,4.10^6	141-6,4.10^6	181-1,6.10^6
23-10^7	63-1,3.10^6	103-2,1.10^6	143-3,5.10^5	183-8,6.10^6
25-7.10^6	65-6,6.10^5	105-6,1.10^6	145-1,5.10^5	185-2.10^6
27-8.10^5	67-6,5.10^5	107-5.10^5	147-1,1.10^6	187-10^6
29-7,9.10^5	69-3,5.10^6	109-3,1.10^6	149-7,2.10^6	189-1,1.10^7
31-5,5.10^6	71-4,2.10^6	111-3,8.10^6	151-5,7.10^6	191-2.10^5

33-2,7.10^6	73-1,3.10^6	113-5,3.10^6	153-6,6.10^6	193-2,9.10^6
35-5,4.10^6	75-3,9.10^6	115-1,6.10^7	155-3,8.10^6	195-3,3.10^6
37-3,1.10^6	77-1,4.10^6	117-9,8.10^6	157 - 10^4	197-3,7.10^6
39-2,3.10^6	79-6,5.10^6	119-1,6.10^6	159-7,8.10^5	199-1,4.10^6

Таблица 1.

В таблице 2 представлены характеристики некоторых множителей, рассмотренных различными авторами: множители 1,2,3 /11/, множители 4,5 - /14/, множители 6,7,8 - /15/. Остальные выбирались произвольно. Первое число в таблице 2 порядковый номер множителя, второе его 0,1 - характеристика, третье - сам множитель, представленный в восьмеричной системе.

Характеристики выбранных множителей λ находятся в пределах от 1 (№ 1, № 3 таблицы 1, № 8 таблицы 2), 907 (№ 179 таблицы 1) до 1,7.10^7 (№ 26 таблицы 2) и 2.10^7 (№ 51 таблицы 1). Среднее значение 0,1 - характеристики близко к 4.10^6.

1-1,3.10^6	11-6,5.10^5	21-1,6.10^5	31-3,8.10^6	41-6,8.10^6
27367316315 5	000001000005	000020000005	406140133735	023706643415
2-7,9.10^6	12-8,1.10^5	22-3,3.10^6	32-4,2.10^6	42-8.10^6
074052161255	000000400005	000040000005	346642505025	010610253515
3-4,6.10^6	13-3,8.10^6	23-4,1.10^6	33-1,1.10^6	43-3,2.10^6
162571342215	000000200005	000003000005	317131175325	003013036255
4-5,4.10^6	14-4,6.10^6	24-1,6.10^6	34-7.10^5	44-1,7.10^6
064256500425	000000100005	000005000005	110765432105	030130362505
5-1,8.10^6	15-2,9.10^6	25-8,1.10^4	35-2,3.10^6	45-1,2.10^6
543660414035	000000040005	000007000005	121176543215	027010036275
6 - 10^7	16-7,1.10^6	26-1,7.10^7	36-9.10^5	46-2,7.10^6
430174170715	000000020005	000011000005	617012345675	270100362705
7-5,1.10^6	17 - 10^6	27-6,6.10^5	37-4,6.10^6	47-1,1.10^6
770037016145	000000010005	000013000005	416135702465	022012036565
8 - 1	18-7,8.10^6	28-5,1.10^5	38-3,3.10^6	48-9,4.10^6
252525252525	000002000005	000015000005	517024613575	220120365605
9-4,9.10^6	19-1,5.10^7	29-6,1.10^6	39-1,5.10^6	49-7,5.10^5
000020367215	000004000005	000017000005	144312011415	003501036625
10-7,3.10^5	20 - 10^6	30-1,1.10^7	40-2,5.10^6	50-1,8.10^6
224102350555	000010000005	224455777405	327251773105	035010366205

Таблица 2.

В таблице 3 дано последовательное получение множителей, обладающих все большими 0,1 – характеристиками. К сожалению, оптимального множителя λ получить не удалось из-за недостатка машинного времени; однако был найден множитель λ с 0,1 – характеристикой, большей, чем у какого-либо из 150 проверенных множителей. Так как во всех рассмотренных случаях 0.1 – характеристика не превосходит величины 2^{26}, поэтому в соответствии со следствием 2.6 корреляционный коэффициент $\rho(2^{P-2}, \lambda^{2^5})$ не больше величины $1/4^{36-4-26} = 1/2^{12} < \frac{1}{1000}$.

1-9.10^5	6-1,2.10^7	11-1,6.10^7	16-2,1.10^7	21-2,6.10^7
021452235075	370163160325	051132716055	440422031765	155205653325
2-1,9.10^6	7-1,2.10^7	12-1,7.10^7	17-2,2.10^7	22-2,8.10^7
323160475745	703450320145	452026500645	312774500005	612656525405
3-2,9.10^6	8-1,3.10^7	13-1,8.10^7	18-2,2.10^7	23-3,5.10^7
153155077045	317643625225	006001537245	546613620755	351244626615
4-3,8.10^6	9-1,3.10^7	14-1,9.10^7	19-2,3.10^7	24-3,6.10^7
522523146315	060525605635	030513064515	566264634105	512467203715
5-7.10^6	10-1,4.10^7	15-2.10^7	20-2,4.10^7	25-3,7.10^7
000555102615	340071323575	177434763625	761270215715	261047521715

Таблица 3.

В данной работе подробно рассмотрен и проверен случай $\ell = 0.1$. Еще больший интерес представляют случаи меньших ℓ. Согласно теорем 2.3, 2.4 и 3.4 величина $\ell/100$ не может быть меньше $1/\sqrt{2^{P-2}}$. Для $P = 36$ наименьшее ℓ порядка 0.001, но уже при $\ell = 0.01$ число множителей, не соответствующих ℓ-уровню возрастает (в соответствии с теоремами 2.3, 2.4 и 3.4) до 8-10 тысяч, а при $\ell = 0.001$ число множителей приблизительно равно

100–120 тысяч. Соответственно возрастают трудности и машинное время получения оптимальных множителей, характеристик и оценки λ. Соответственно уменьшаются и ℓ – характеристики.

Если для некоторой задачи нужно не слишком много псевдослучайных чисел, то можно, задавшись ℓ, найти подходящий множитель. Если наибольшая ℓ –характеристика меньше требуемого количества псевдослучайных чисел, то можно представить интересующую нас выборку псевдослучайных чисел Q как сумму ℓ –характеристик $L(\lambda_i)$:

$$Q \leqslant L(\lambda_1) + L(\lambda_2) + \ldots + L(\lambda_n)$$

Таким способом можно получать псевдопоследовательности любой (практически) длины в высокой степени отвечающие критериям случайности.

В заключение кратко перечислим основные результаты работы.

В главе 1 показано, что операция умножения наилучшим образом отвечает требованиям, предъявляемым датчикам псевдослучайных чисел для ЭВМ.

В главе 2 введено понятие эквивалентности датчиков и показано, что датчики смешанного и несмешанного типов с одним и тем же множителем эквивалентны. При помощи алгоритма Евклида для датчика $x_{i+1} \equiv \lambda x_i (mod\, 2^P)$ получена формула корреляционного коэффициента (теорема 2.1), довольно просто реализуемая на ЭВМ.

В главе 3 на основе теории групп рассматриваются семейства множителей λ и находится количество этих семейств (теоремы 3.1 – 3.3). На основе теорем 2.3, 2.4 и 3.4 найдены все семейства, превосходящие заданный ℓ –уровень. ℓ – характеристику можно получить пользуясь результатами теоремы 3.5, а оптимальную ℓ –характеристику и семейство из теоремы 3.6.

В главе 4 предлагается некоторое преобразование, с помощью которого можно получать псевдослучайные числа, пригодные для использования в качестве логической шкалы.

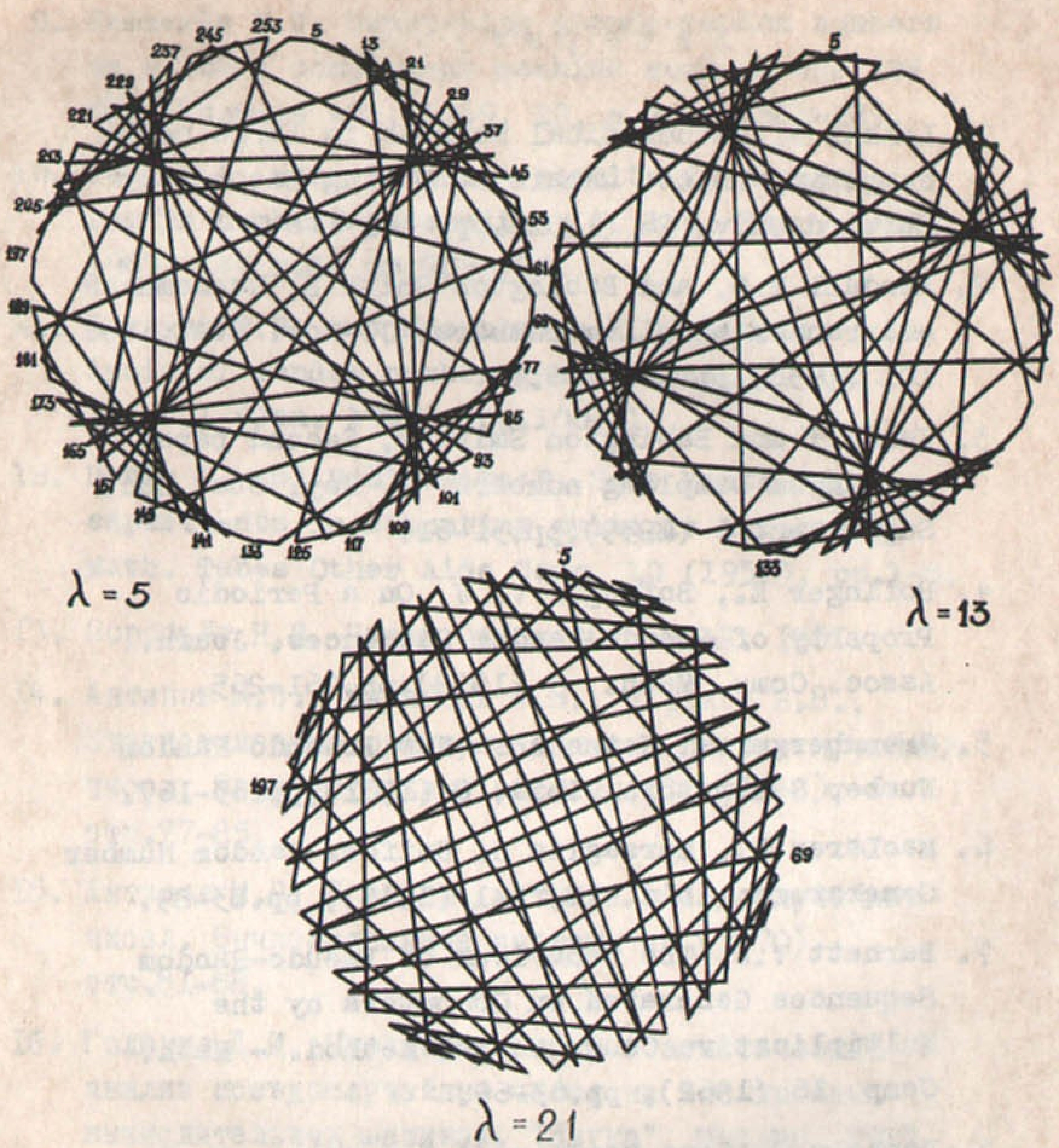

Рис.1. Полные периоды последовательностей для Р = 8.

Литература

1. Lehmer D. Mathematical methods in large scale computing units. Annals Computing Laboratory Harvard Univ. 26 (1951),pp. 141-146.
2. Kendall M.G. and Babington Smith B. Randomness and random sampling numbers, J. Roy. Stat. Soc. 101 (1938),pp.147-166.
3. Kendall and Babington Smith B, Second paper on random sampling numbers, J. Roy. Stat.Soc. Supplement 6 (1939),pp.51-61.
4. Bofinger E., Bofinger V. J. On a Periodic Property of Pseudo-Random Sequences. Journ. Assoc. Comp. Mach., 5 (1958),pp.261-265.
5. Greenberger M. Notes on a New Presudo-Random Number Generators. ibid. 8 (1961),pp163-167.
6. MacLaren D., Marsaglia G. Uniform Random Number Generators. ibid. 12, n.1 (1965), pp.83-89.
7. Barnett V.D. The Behaviour of Pseudo-Random Sequences Generated on Computers by the Multiplicative Congruential Method. - Math. Comp. 16 (1962), pp.63-69.
8. Donnely T. Some techniques for using pseudo-random numbers in computer simulation, Communs ACM, 1969, 12, n.7, pp.392-394.
9. Hemmerle W.J. Generating pseudo-random numbers on a two's complement machine such as the IBM 360. Communs ACM, 1969, 12, n.7, pp.382-383.
10. Gelder A. van, Some new results in pseudo-random numbers generation. J. Ass. Comp. Mach. 1967, 14, n.4, pp.785-792.
11. Coveyou R.R. and Macpherson R.D. Fourier analysis of random number generations. J. ACM. 14, n.1 (Jan. 1967), pp.100-119.
12. Davis P. and Rabinowitz P. Some Monte-Carlo experiments in computing multiple integrals. Math. Tabes Other Aids Comp. 10 (1956), pp.1-8.
13. Воробьёв Н.Н. Числа Фибоначчи. М.-Л. 1951.
14. Антипов М.В., Израйлев Ф.М., Чириков Б.В., Статистическая проверка датчика псевдослучайных чисел. Вычислительные системы, 30 (1968), стр.77-85.
15. Антипов М.В. К оценке датчика псевдослучайных чисел. Вычислительные системы 42 (1970), стр.81-88.
16. Голенко Д.И. Моделирование и статистический анализ псевдослучайных чисел на электронных вычислительных машинах. "Наука", Москва, 1965.