С.Л. Василенко

"Золотой" генератор псевдослучайных чисел

Генерация случайных чисел слишком важна,
чтобы оставлять её на волю случая...
Роберт Кавью [1]

Введение. Случайные числа широко используются в самых разных приложениях современной информатики: в вычислительных методах, имитационном моделировании (Монте-Карло), системах защиты информации и др. Их генерирование – одна из базовых проблем в реализации криптографических систем, ибо только абсолютно случайное число может рассматриваться в качестве надежного синтезатора безупречного ключа [2, 3].

Шифрование применялось еще в античности. А «краткое руководство по использованию шифров для обмена любовными посланиями содержит даже Камасутра» [4].

Но преобразование информации долгое время носило в основном детерминированный характер. Современные шифры уже содержат случайные (хаотические) компоненты. И как ни странно, но уязвимость многих реальных систем криптографической защиты информации очень часто зависит именно от способа генерирования случайных чисел [5].

Идеальным источником энтропии являются результаты измерения физических величин, имеющие доказуемо случайное поведение, например, источники теплового шума, счетчики Гейгера и др. Но чаще всего соответствующие физические датчики недоступны либо применение дополнительного оборудования затруднительно.

Тогда прибегают к алгоритмическим приемам на вычислительных машинах.

Компьютеры конструктивно относятся к детерминированным системам, поэтому синтез случайных чисел на них не является тривиальной задачей [6].

В современных ЭВМ имеются аппаратные или программные средства для генерирования случайных чисел, которые симулируют хаотический процесс с равномерным законом распределения и являются важнейшим криптографическим примитивом. Имитируемые последовательности, хотя и детерминированные, их статистические свойства по определенным критериям близки к характеристикам случайных чисел.

Наиболее распространенным классом таких генераторов являются рекуррентные аналоги. Они формируют числовые последовательности, в которых каждый член зависит от одного или нескольких предыдущих. При этом весь ряд зависит от начального (порождающего) числа или группы таких чисел. В отношениях между кодировщиком и злоумышленником-взломщиком это слабая сторона. Для иных случаев, таких как многократное воспроизведение эксперимента, наоборот достоинство.

Системы безопасности требуют наличия специальных последовательностей, которые не только похожи на случайные ряды и удовлетворяют различным тестам, но и обладают свойством непредсказуемости.

В других задачах последнее вовсе не обязательно.

Постановка задачи. В последнее время достигнуты определенные успехи в части разработки устойчивых генераторов случайных (псевдослучайных) чисел[1] (ГСЧ).

Этот процесс особенно интенсифицировался с развитием компьютерной техники и криптографии. Повышенные требования к защите информации и шифровальным процедурам потребовали формирования числовых последовательностей с очень большими периодами.

---

[1] Алгоритм, генерирующий последовательность псевдослучайных чисел, почти независимых друг от друга и подчиняющихся заданному распределению, обычно равномерному с равными вероятностями.

Для выявления возможных отклонений от случайности синтезируются эффективные статистические тесты [7], основанные на методах теории информации.

Вместе с тем во многих практических приложениях или исследовательских задачах часто возникает необходимость использования коротких псевдослучайных выборок.

Причем с достаточно высокими требованиями, например, к той же равномерности распределения чисел на выбранном интервале.

Так, при обработке данных часто очень важен беспристрастный выбор n случайных записей из файла, содержащего N записей. Подобная задача появляется, в частности, при контроле качества или других статистических вычислениях [8, п.3.4.2].

Но что интересно, суперсовременные генераторы, рассчитанные на синтез непериодических последовательностей чрезвычайно большой длины, на малых выборках очень часто неэффективны. В том смысле, что сформированные наборы чисел весьма далеки от требуемых свойств. Например, время от времени они могут сбиваться (группироваться) слева или справа от моды распределения и своим выборочным средним существенно отклоняться от середины отрезка.

Можно, конечно, вероятностные характеристики выборок подбирать путём многократного повторения рекуррентных процедур, выходя на априори заданные параметры.

Но это не всегда удобно при проведении инженерных расчетов и требует достаточно высокой квалификации. Решение практических вычислительных задач с применением случайных чисел существенно упрощается с одновременным повышением достоверности результатов, когда исследователь особо не задумывается о качестве исходных чисел, а всё внимание сосредотачивает на основной проблеме. И здесь весьма полезными оказываются ГСЧ, способные воспроизводить случайные выборки небольшой длины, максимально приближенные к непрерывному равномерному распределению, из которого уже потом с помощью отдельных процедур можно получать и прочие распределения: нормальные и др.

Целью работы является алгоритмизация генерирования равномерно распределенных псевдослучайных чисел на основе золотого сечения (ЗС).

Генерация случайной последовательности с произвольным законом распределения также сводится к генерации равномерно распределенной случайной последовательности.

Исторические параллели. Алгоритмы ГСЧ постоянно совершенствуются и усложняются, хотя в своей основе всё так же содержат разные модификации рекуррентных соотношений [8, п.3.2], которые известны более полувека.

Так, Д.Кнут отмечает [8, п.3.2.2], что рекуррентный ГСЧ $x_n = \left(x_{n-1} + x_{n-p}\right) \bmod m$, основанный на обобщенной последовательности Фибоначчи, был введен ещё в 1959 г.[2]

Числа, определяемые соотношением $x_{n+1} = x_{n-k} + x_{n-p}$, обычно называют последовательностью Фибоначчи с запаздыванием (k, p). Они были весьма востребованы и успешно применялись в качестве генераторов случайных чисел уже в конце 50-х годов прошлого столетия.

Рекуррентная форма $x_n = x_{n-1} + x_{n-p}$, как "уравнение в *конечных разностях*", представлена математиком Д.Пойа [9, с. 114, с. 393], о чем подробно описано в статье [10].

Последнее также относится к линейным возвратным (разностным) однородным уравнениям с постоянными коэффициентами [11, с. 329–347], имея адекватное алгебраическое представление (характеристическое уравнение) [11, с. 330]: $x^p = x^{p-1} + 1$.

Заметим, что некоторые авторы продолжают по второму и третьему кругу "переоткрывать" данные (известные более полувека) последовательности, в частности, называя p-числами Фибоначчи.

---

[2] Green, Smith, Klem / JACM, **6**, 1959, 527–537. / 2-й том Кнута вышел в издательстве "Мир" в 1977 г.

Кроме того, известны случаи, когда их произвольно наделяют свойствами единственной в своём роде золотой пропорции, называя корни характеристических полиномиальных уравнений "золотыми p-сечениями" [12, с. 192–202]. Подобная практика в математике не считается приемлемой, поскольку противоречит закономерностям логики [13, с. 395]. Ведь обобщение понятий подразумевает исключение видового признака, а образуемое новое понятие имеет более широкий смысл, но менее конкретное содержание.

Что касается самих рекуррентных числовых последовательностей, то они нисколько не устарели и в разных модификациях продолжают служить надежным источником случайных чисел, используемых в разнообразных технических устройствах, не обязательно в качестве криптографических примитивов.

Так, в работе [14] описывается метод построения ГСЧ на основе линейно-рекуррентной последовательности p-чисел Фибоначчи $F_n = F_{n-1} + F_{n-p}$ для формирования переменной несущей частоты широтно-импульсной модуляции. В частности, используется трином $x^{22} - x^{21} - 1$ для ГСЧ 12-разрядных чисел. Метод характеризуется достаточной величиной периода повторяемости (более 4 млн), высокой скоростью генерирования чисел и достаточно хорошими статистическими характеристиками.

Основные предпосылки. «В математике не принято давать "металлические" названия, если не считать одно единственное исключение» [15, с. 50]: уникальное "золотое" деление единичного отрезка в геометрии с его большей частью, равной $\phi = \left(\sqrt{5}-1\right)/2$.

Это алгебраическое иррациональное число.

Оно не может быть представлено в виде отношения двух натуральных чисел и записывается в виде непериодической бесконечной десятичной дроби.

Значит, для любого натурального n произведение $n \cdot \phi$ отлично от целого.

Число золотого сечения $\Phi = \left(\sqrt{5}+1\right)/2 = \phi^{-1}$, как корень квадратного уравнения $x^2 = x + 1$, превращает его в тождество $\Phi^2 = \Phi + 1$, непосредственно из которого (после деления на Ф) путем многократного повторения следует редкостное разложение в бесконечную цепную дробь, состоящую из одних единиц

$$\Phi = 1 + \frac{1}{\Phi} = 1 + \phi = 1 + \frac{1}{1 + \frac{1}{\Phi}} \approx 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \ldots}}}.$$

Существуют и другие, не менее интересные разложения Ф [16], но вот подобный феномен через единичное представление не свойственен больше никакому числу!

На наш взгляд, именно это свойство является базовым в алгоритме "золотого" ГСЧ.

Описание алгоритма. Образуем бесконечную последовательность величин, кратных ϕ

$$z_n = \{n \cdot \phi\}, \quad n = 1, 2, 3\ldots$$

Ни одно из чисел z_n не имеет дробной части d_n, равной нулю, и никакие два числа не имеют одинаковых дробных частей [15, с. 51].

Выберем из последовательности $\{z_n\}$ первые N чисел.

Сформируем матрицу A размером $N \times 2$: $A_{n,1} = n.$; $A_{n,2} = d_n$.

Выполним сортировку строк матрицы A выстраиванием элементов 2-го столбца в порядке возрастания.

В первом столбце по-прежнему будут находиться все числа от 1 до N.

Только теперь они расположены не в порядке возрастания, а преимущественно случайным образом с равномерной функцией распределения (табл. 1).

Таблица 1

Псевдослучайные числа с равномерной плотностью распределения, сформированные в соответствии с дробной частью золотого сечения

$N = 100$

89	**34**	68	13	47	81	26	60	05	94	39	73	18	52	86	31	65	10	99	44
78	23	57	02	91	36	70	15	49	83	28	62	07	96	41	75	20	54	88	33
67	12	46	80	25	59	04	93	38	72	17	51	85	30	64	09	98	43	77	22
56	01	90	35	69	14	48	82	27	61	06	95	40	74	19	53	87	32	66	11
100	45	79	24	58	03	92	37	71	16	50	84	29	63	08	97	42	76	**21**	**55**

$N = 1\,000$

610	**233**	843	466	089	699	322	932	555	178
788	411	034	644	267	877	500	123	733	356
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
254	864	487	110	720	343	953	576	199	809
432	055	665	288	898	521	144	754	**377**	**987**

$N = 10\,000$

4181	8362	**1597**	5778	9959	3194	7375	0610	4791	8972
2207	6388	3804	7985	1220	5401	9582	2817	6998	0233
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
6532	3948	8129	1364	5545	9726	2961	7142	0377	4558
8739	1974	6155	3571	7752	0987	5168	9349	**2584**	**6765**

$N = 100\,000$

75025	**28657**	57314	10946	85971	39603	68260	21892	96917	50549
04181	79206	32838	61495	15127	90152	43784	72441	26073	54730
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
95320	48952	02584	77609	31241	59898	13530	88555	42187	70844
24476	99501	53133	06765	81790	35422	64079	**17711**	92736	**46368**

Терминологические казусы. В работе [15, с. 50–51] подобный массив чисел при $N = 10\,000$ назван "железной таблицей". Это повторяется и в монографии [12, с. 75–77].

Однако, учитывая традиционное отсутствие в математике какого-либо упоминания или стремления давать "металлические" наименования, такая железная металлизация не может считаться корректно-приемлемой.

Более подходящим, на наш взгляд, названием здесь можно считать привычный термин «генератор (таблица) псевдослучайных целых чисел». Можно даже использовать и образную интерпретацию, как "золотой рог изобилия" равномерно распределенных случайных чисел.

Слово "золотой" здесь отражает метод получения чисел с использованием ЗС, а потому вполне допустимо. Чего нельзя сказать о другом аспекте терминологических вольностей.

Так, Г.Штейнгауз чисто волюнтаристическим образом называет ряд чисел, кратных Ф, последовательностью золотых чисел [15, с. 50]. Это, конечно, привносит путаницу и неразбериху в математические определения, в конечном итоге символизируя бессмысленность, ибо золотые числа (Φ, ϕ) в математике уже есть.

Мы же не называем $10 \cdot \pi$ или π^2 π-числами?

Тогда откуда такое своеволие при обращении с научным понятием ЗС?

Неотрадно и другое. Вместо того чтобы "бить тревогу" и аргументировано оппонировать, ибо де-факто нивелируется понятийная и теоретическая основа ЗС, тема псевдозолочения без тени сомнения наоборот подхватывается [12, с. 76].

Хотя невооруженным глазом видно, что подобные терминологические позолоты бесконечного множества конкретных чисел не усиливают, а напротив, ослабляют имидж, а также и без того не очень стабильные позиции ЗС в науке.

Краткое обсуждение. Примечательно, что все примеры из табл. 1 начинаются и заканчиваются числами Фибоначчи $F_n = F_{n-1} + F_{n-2}$, $(F_0, F_1) = (0, 1)$.

Объяснение этому факту очень простое: величины

$$\phi F_n = \phi \frac{\Phi^n - (-1)^n \Phi^{-n}}{\sqrt{5}} = \frac{\Phi^{n-1} + (-\phi)^{n+1}}{\sqrt{5}}$$

максимально приближены к целым числам, и в результате ранжирования дробных частей они автоматически попадают на края монотонно возрастающей последовательности.

Так, $\phi F_{20} = 4180{,}99993$; $\phi F_{21} = 6765{,}00004$.

Неоспоримым преимуществом "золотого" генератора является способность образовывать небольшие выборки случайных чисел, равномерно распределенных на заданном интервале, что непосредственно следует из характера последовательностей (рис.1).

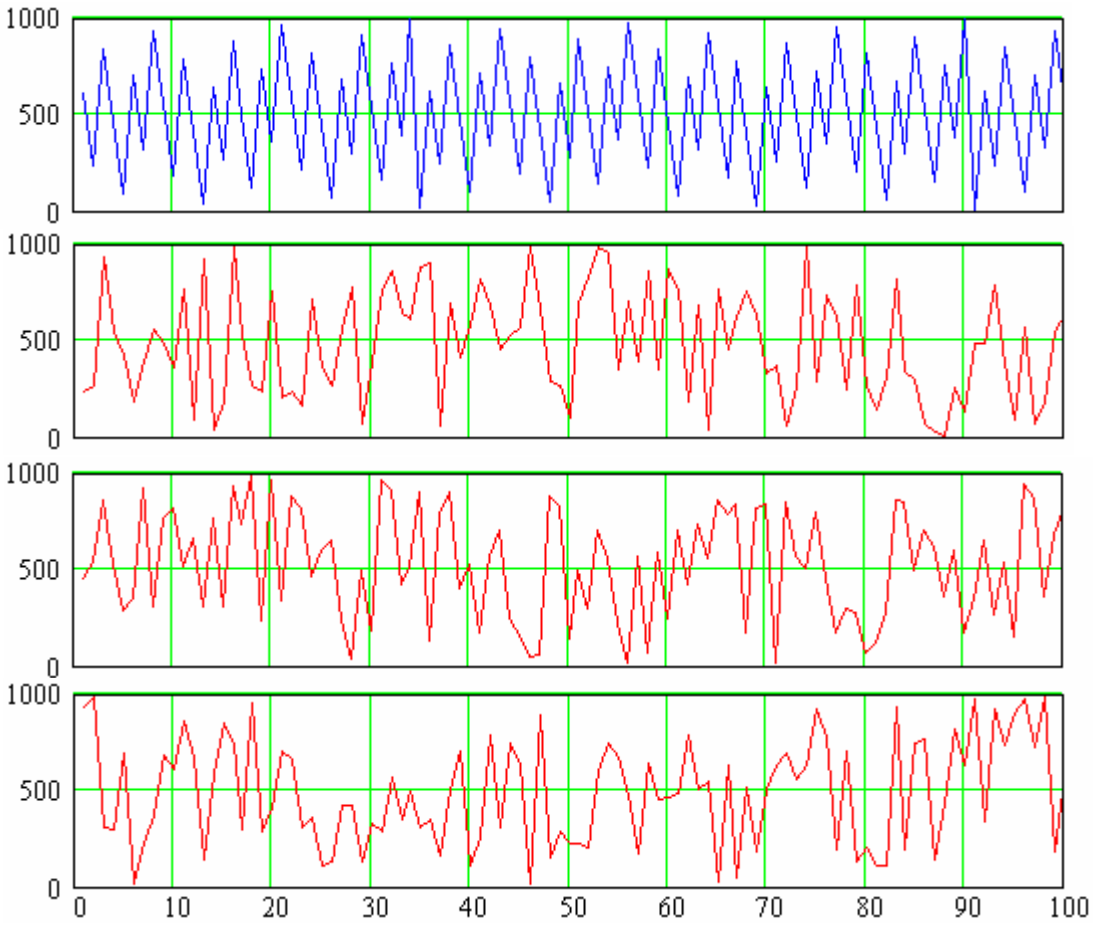

Рис. 1. Выборки псевдослучайных чисел с равномерной плотностью распределения:
вверху – с помощью "золотого генератора"
нижние три графика – компьютерная программа Randu в среде MathCad

В каком бы месте мы не вырезали ограниченную выборку (рис. 1, верхний график), она удивительным образом формирует, хотя и случайное, но достаточно равномерное заполнение интервала, в котором варьирует переменная (случайная функция).

Тестирование. Проверка свойств исследуемых последовательностей осуществляется с помощью разнообразных тестов: графических, статистических и др. [7, 17], ассортимент которых постоянно пополняется. Мы не будем их все исследовать или применять.

Так, гистограмма распределения элементов ряда, позволяющая оценить равномерность распределения чисел (символов) в последовательности и определить частоту их повторения, для "золотого" генератора не требуется. – Никакие натуральные числа в нашей последовательности не повторяются.

Одним из тестов для определения равномерности является *проверка на монотонность*, исходя из анализа отсортированных неубывающих подпоследовательностей.

Простая визуальная проверка (рис. 2) показывает высокую эффективность "золотого" генератора: случайные числа выстраиваются равномерно (достаточно близко по диагонали).

Плотность распределения практически линейна.

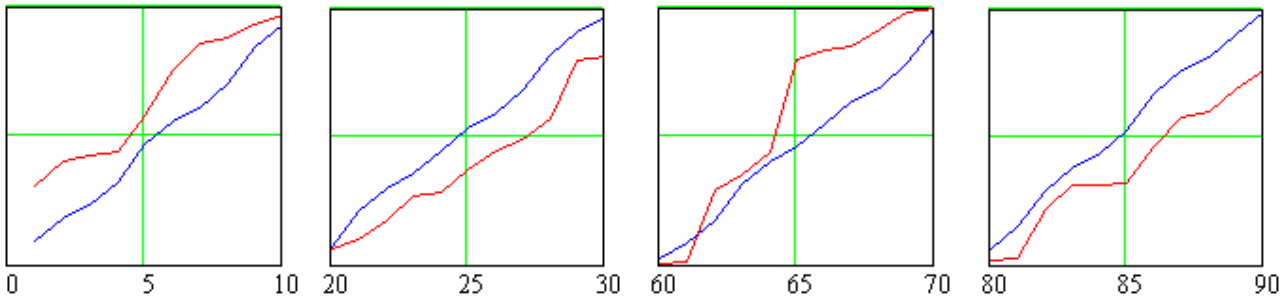

Рис. 2. Проверка монотонности упорядоченных выборок (по 10 значений) псевдослучайных чисел с равномерной плотностью распределения

Алгоритмические закономерности. Благодаря уникальным свойствам ЗС и чисел Фибоначчи формирование таблицы случайных чисел происходит не совсем хаотически, а подчиняется определенным детерминистическим правилам. Они сравнительно легко узнаваемы и устанавливаются путем анализа взаимосвязей при последовательном увеличении размерности вектора псевдослучайных чисел (табл. 2).

Таблица 2

Порядок последовательного расширения вектора псевдослучайных чисел

	N																			
F_6	**8**	5	2	7	4	1	6	3	**8**											
	9	5	2	7	4	**9**	1	6	3	8										
	10	5	**10**	2	7	4	9	1	6	3	8									
	11	5	10	2	7	4	9	1	6	**11**	3	8								
	12	5	10	2	7	**12**	4	9	1	6	11	3	8							
F_7	**13**	**13**	5	10	2	7	12	4	9	1	6	11	3	8						
	14	13	5	10	2	7	12	4	9	1	**14**	6	11	3	8					
	15	13	5	10	2	**15**	7	12	4	9	1	14	6	11	3	8				
	16	13	5	10	2	15	7	12	4	9	1	14	6	11	3	**16**	8			
	17	13	5	10	2	15	7	12	4	**17**	9	1	14	6	11	3	16	8		
	18	13	5	**18**	10	2	15	7	12	4	17	9	1	14	6	11	3	16	8	
	19	13	5	18	10	2	15	7	12	4	17	9	1	14	6	**19**	11	3	16	8
	20	13	5	18	10	2	15	7	**20**	12	4	17	9	1	14	6	19	11	3	16	8
F_8	**21**	13	5	18	10	2	15	7	20	12	4	17	9	1	14	6	19	11	3	16	8	**21**

Так, при $N = 8 = F_6$ ряд случайных чисел имеет вид: 5, 2, 7, 4, 1, 6, 3, 8.

Следующее число $F_6 + 1 = 9$ "раздвигает строку и встраивается" на место единицы, 10 – на позицию двойки, 11 – вместо тройки и так далее: всего $F_7 - 1 = F_8 - F_6 - 1 = 12$ раз.

Последнее число $F_8 = 21$ занимает правую крайнюю ячейку вектора-строки.

Далее процедура повторяется для следующей пары чисел Фибоначчи с чётными индексами.

Программная реализация чрезвычайно проста, однако не эффективна, поскольку вычисления требуют много времени, что вызвано поиском на каждом шаге местонахождении (позиции) необходимого числа в длинной последовательности, размерность которой постоянно возрастает.

Так что данные закономерности имеют скорее академическое значение, нежели практическое применение, – разве что при рекурсивной достройке имеющейся таблицы.

Но рекуррентно-циклические свойства всё ж имеют место.

Они легко просматриваются, если длину последовательности случайных чисел определять числами Фибоначчи.

В частности, несомненный интерес представляет выявленная нами закономерность при построении вектора случайных чисел размерностью, равной числу Фибоначчи F_n.

При фиксированном значении n вектор v длиной F_n формируется по простой схеме:

$$v_{tF_{n-1} \pmod{F_n} + c} = t\,, \tag{1}$$

$$v_1 = F_n \quad \text{if} \quad d = 1, \qquad v_b = F_n \quad \text{if} \quad d = 0\,,$$

где $c = n \pmod 2$, $t = \overline{1, F_n - 1}$.

```
GoldG(n) := | (a  b  c) ← (F_{n-1}  F_n  mod(n,2))
            | for t ∈ 1..b − 1
            |   v_{mod(t·a,b)+c} ← t
            | v_1 ← b  if c = 1
            | v_b ← b  otherwise
            | v
GoldG(6)^T = (0  5  2  7  4  1  6  3  8)
```

Здесь каждое из последовательных натуральных чисел t ставится строго на обусловленное место (вектора v). Надлежащий индекс определяется через взятие по модулю F_n произведения tF_{n-1}.

Такой алгоритм гарантированно сходится для любого натурального n.

Это непосредственно следует из того, что «соседние числа Фибоначчи взаимно просты» [18, с. 45], то есть, у них нет общих делителей[3], кроме 1. Действительно, если F_{n-1}, F_n имеют общий делитель $d > 1$, то и разность $F_n - F_{n-1} = F_{n-2}$ делится на d, а значит, по индукции делятся на d и числа $F_{n-3}, F_{n-4} \ldots F_1 = 1$, что приводит к противоречию.

Выше в необходимых ячейках последовательно расставлялись натуральные числа от 1 до F_n. Но такую расстановку можно осуществлять и в несколько ином порядке, например

$$v_{tF_{n-z} \pmod{F_n} + d} = tF_z \pmod{F_n}. \tag{2}$$

Необходимым условием здесь является: нечетность $z = 2m + 1 < n$ и взаимная простота пары чисел $\gcd(z, n) = 1$.

Вообще-то, строго говоря, требуется взаимная простота чисел Фибоначчи, но хорошо известно [18, с. 46], что F_z делится на F_n тогда и только тогда, когда z делится на n. Поэтому о делимости чисел Фибоначчи можно судить по делимости их порядковых номеров.

---

[3] Наибольший общий делитель (НОД) равен $\gcd(F_n, F_{n-1}) = 1$.

Соотношение (2) – более общее и включает в себя (1) при $z = 1$, то есть оно отличается многообразием формирования массива псевдослучайных чисел.

Но можно пойти и по пути некоторого упрощения вычислительной процедуры и ее представления в более привычном для нас рекуррентном виде с последовательным нарастанием нижнего индекса:

$$v_{t+1} = (v_t + a) (\mathrm{mod}\ F_n), \tag{3}$$

где начальные условия определяются по четности-нечетности числа n

$$\begin{cases} (v_1, a) = (F_{n-1}, F_{n-1}), & n = 2s; \\ (v_1, a) = (F_n, F_{n-2}), & n = 2s+1. \end{cases}$$

Из рассмотренных вариантов это, пожалуй, наиболее простая и удобная для реализации рекуррентная форма.

На краях вектора-массива v находятся соседние числа Фибоначчи так, что для нечетных значений n концы интервала замыкают числа (F_n, F_{n-1}), для четных значений n – числа (F_{n-1}, F_n). Например, $n = 5$: $v = (\mathbf{5}\ 2\ 4\ 1\ \mathbf{3})$; $n = 6$: $v = (\mathbf{5}\ 2\ 7\ 4\ 1\ 6\ 3\ \mathbf{8})$.

Анализируя полученные последовательности отдельно для четных и нечетных параметров n, нетрудно отметить похожесть в следовании элементов ряда v в прямом и обратном направлении.

Но формирование данным способом рядов не является догмой, и нам ничего не мешает для нечетных значений n элементы ряда расположить в обратном порядке.

Этим самым мы добиваемся определенной унификации (типизации) в построении последовательностей.

Более того, существенно упрощается запись расчетной формулы, объединяя в себе одновременно черты аналитического и рекуррентного представления:

$$v_t = F_n - tF_{n-2} (\mathrm{mod}\ F_n), \quad t = \overline{1, F_n}. \tag{4}$$

С точки зрения ГСЧ формула (4) замечательна во многих отношениях:

1. Прежде всего, выстраиваемые ряды теперь имеют похожее строение, начиная и заканчиваясь числами (F_{n-1}, F_n).

2. Максимальным значением каждой последовательности является F_n, поэтом нормированные положительные числа v'_t не превышают единицы

$$v'_t = \frac{v_t}{F_n} = 1 - \frac{tF_{n-2} (\mathrm{mod}\ F_n)}{F_n} \le 1.$$

Переходя к пределу $F_{n-2}/F_n \to \phi^2$ и используя тождество $\phi = 1 - \phi^2$, можно как бы вернуться к исходной точке рассуждений, записав генератор бесконечного числа неповторяющихся десятичных чисел, равномерно распределенных на интервале (0, 1) и начинающихся с точного значения числа ЗС $\phi \approx 0{,}618$:

$$v_t = t\phi\ (\mathrm{mod}\, 1) = 1 - t\phi^2\ (\mathrm{mod}\, 1).$$

3. Последовательности обладают интересными свойствами, в частности ($k = 1, 2, 3\ldots$),

$$v_k + v_{F_n - k} = v_{F_n}.$$

4. Период может быть настолько длинным, насколько это необходимо, чем собственно удовлетворяются любые практические потребности.

5. Ряды достаточно хорошо структурированы, имея выраженные признаки организованной хаотичности.

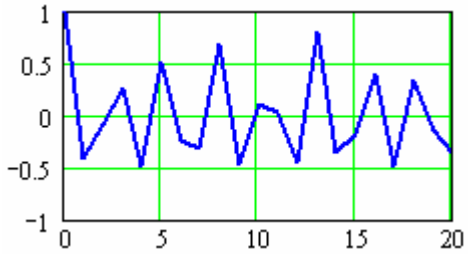

Рис. 3. Автокорреляционная функция "золотого" генератора псевдослучайных чисел

Особо отметим, что подобная структурированность не должна нас нисколько настораживать, ибо мы не собираемся их использовать для скрытых (тайных) шифров. Понятно, что для целей, предполагающих режимы секретности, данные алгоритмы не предназначены.

В то же время автокорреляционная функция (рис. 3) свидетельствует о статистически значимой корреляции чисел. Это и не удивительно, принимая во внимание детерминированный характер алгоритма.

Алгоритмические параллели. Форма (4) структурно напоминает линейные конгруэнтные последовательности, определяемые посредством значений дробной части многочлена первой степени [8, п.3.2.1]

$$x_t = (ax_{t-1} + b) (\mathrm{mod}\ m),$$

где a и b – натуральные числа-константы, x_0 – исходное порождающее число.

Эти три величины образуют ключ.

Значение модуля m обычно устанавливается равным 2^k, где k – длина машинного слова в битах, что позволяет избавиться от относительно медленной операции приведения по модулю.

Если t пробегает значения натурального ряда чисел, то поведение x_t выглядит довольно хаотичным, образуя псевдослучайные числа с периодом повторения T.

Линейный конгруэнтный метод дает максимальную длину $T = m$ если [8]:

– приращение b и модуль m взаимно просты, то есть НОД(b, m) = 1;
– $a - 1$ кратно p для всех простых p – делителей m;
– $a - 1$ кратно 4, если m кратно 4, то есть a(mod 4) = 1.

Понятно, что никакой детерминированный алгоритм не может генерировать полностью случайные числа и дает только аппроксимацию их некоторых свойств.

По мере повышения требований к качеству случайных чисел получило развитие семейство фибоначчиевых алгоритмов [19].

Один из подобных генераторов основан на итеративной формуле:

$$x_t = \Delta_t + \mathbf{1}(-\Delta_t)$$

где $\Delta_t = x_{t-a} - x_{t-b}$, $\mathbf{1}(\xi)$ – единичная функция (Хевисайда), равная {1, $\xi \geq 0$; 0, $\xi < 0$}.

Рекомендуются следующие значения лагов: (a, b) = (55, 24), (17, 5) или (97, 33).

Получаемые случайные числа обладают хорошими статистическими свойствами.

Все биты случайного числа равнозначны по вероятностным характеристикам.

Период датчика оценивается по формуле: $T = \left(2^{\max(a,\, b)} - 1\right) \cdot 2^k$, где k – число битов в мантиссе вещественного числа.

Для старта такому алгоритму требуется max(a, b) случайных чисел, которые могут быть сформированы линейным конгруэнтным генератором.

Заключение и выводы.

В данной работе не ставилась задача повышения надежности криптографических систем. Хотя направленность исследований имеет ярко выраженное прикладное значение.

"Золотой" генератор псевдослучайных равномерно распределенных чисел обладает аналитико-рекуррентной формой и легко реализуется на практике, особенно для последовательностей, длины (периоды) которых равны заданным числам Фибоначчи:

$$v_t = F_n - tF_{n-2} \pmod{F_n}, \quad t = \overline{1, F_n}.$$

Термин "золотой" подчеркивает тот факт, что отношение крайних членов последовательности (F_{n-1}, F_n) стремится к числу золотого сечения Φ.

Простота алгоритма в данном случае не есть его ущербность, а наоборот высвечивает преимущество, ибо сложный алгоритм ещё не означает хороший генератор.

Главным достоинством "золотого" ГСЧ является *монотонность* отсортированных неубывающих подпоследовательностей. – Значит, для отдельных коротких выборок их среднее и мода во всех случаях будут максимально приближены к середине интервала.

Метод характеризуется простотой реализацией и приемлемыми статистическими характеристиками случайных чисел.

К отрицательным моментам подобных псевдослучайных рядов следует отнести статистическую значимость значений автокорреляционной функции, что ограничивает их эффективное использование в динамических структурах.

Можно сказать, что здесь присутствует структурированная или хорошо организованная (спланированная) хаотичность. Детерминированного здесь явно больше чисто случайного.

В целом числовые последовательности, сформированные "золотым" генератором, практически самоподобны отдельным своим структурным выборкам. Это означает, что вырезанные случайным образом небольшие совокупности исходных данных довольно точно (в статистическом смысле) воспроизводят (повторяют) свойства генеральной выборки.

Разработанный метод формирования псевдослучайных чисел может также оказать незаменимую пользу при воспроизведении повторяющихся числовых экспериментов.

Литература.

1. *Блох А*. Закон Мерфи: Пер. с англ. – М.: Попурри, 2003. – 224 с.
2. *Кибардин А.В*. Математические методы криптографии. – Екатеринбург: УГТУ–УПИ, 2008. – 33 с.
3. *Баричев С.Г., Гончаров В.В., Серов Р.Е*. Основы современной криптографии. – М.: Горячая линия–Телеком, 2002. – 175 с.
4. *Николенко С.И*. Новые конструкции криптографических примитивов, основанные на полугруппах, группах и линейной алгебре: Дис. ...канд. физ.-мат. наук: 01.01.06. – СбП., 2008. – 120 с. – http://logic.pdmi.ras.ru/~sergey/papers/Nikolenko_PhDThesis.pdf.
5. *Интернет*-сайт Security Lab. – http://www.securitylab.ru.
6. *Харин Ю.С., Ярмола А.Н., Петлицкий А.И*. Методы и алгоритмы статистического тестирования генераторов случайных и псевдослучайных последовательностей в системах информационной безопасности // Искусственный интеллект. – 2006. – № 3. – С. 793–803. – http://iai.dn.ua/public/JournalAI_2006_3/Razdel10/14_Kharin_Yarmola_Petlitskiy.pdf.
7. *Rukhin A. and others*. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 (with revisions dated May 15, 2001). – http://csrc.nist.gov/rng/SP800-22b.pdf.
8. *Кнут Д.Е*. Искусство программирования. Т 2. Получисленные алгоритмы: – 3-е изд. – М.: "Вильямс", 2007. – 832 с.
9. *Пойа Д*. Математическое открытие: Пер. с англ. – М.: Наука, 1970. – 452 с.

10. *Василенко С.Л.* В поисках золотника // Академия Тринитаризма. – М.: Эл. № 77-6567, публ.15629, 03.11.2009. – http://www.trinitas.ru/rus/doc/0016/001c/00161569.htm.

11. *Гельфонд А.О.* Исчисление конечных разностей: Учеб. пособие. – 4-е изд., стер. – М.: КомКнига, 2006. – 376 с. (2-е изд. – 1959)

12. *Stakhov A.* Mathematics of Harmony: from Euclid to Contemporary Mathematics and Computer Science. – World Scientific Publishing Company, 2009. – 748 p.

13. *Кондаков Н.И.* Логический словарь-справочник: 2-е изд. – М.: Наука, 1975. – 720 с.

14. *Уфимцева В.Б.* Генератор псевдослучайных чисел на основе *p*-чисел Фибоначчи для формирования широтно-импульсной модуляции // Коммунальное хозяйство городов. – 2003. – Вып. 49. – С. 174–178. – http://eprints.kname.edu.ua/2925/.

15. *Штейнгауз Г.* Задачи и размышления: Пер. с польск. – М.: Мир, 1974. – 400 с. – http://lib.org.by/_djvu/M_Mathematics/.

16. *Василенко С.Л.* Златые цепи // Академия Тринитаризма. – М.: Эл. № 77-6567, публ.15557, 22.09.2009. – http://www.trinitas.ru/rus/doc/0016/001c/00161546.htm.

17. *Тестирование* псевдослучайных последовательностей // Википедия. Дата обновления: 14.08.2010. – http://ru.wikipedia.org/?oldid=26965046.

18. *Воробьев Н.Н.* Числа Фибоначчи: 4-е изд., доп. – М.: Наука, 1978. – 144 с.

19. *Метод* Фибоначчи с запаздываниями // Википедия Д.Уэйлса. Дата обновления: 13.04.2010. – http://ru.wikipedia.org/?oldid=23743127.