ЧЕБЫШЕВСКИЙ СБОРНИК
Том 26. Выпуск 4.

УДК: 511.36 DOI: 10.22405/2226-8383-2025-26-4-454-460

О подходе к построению последовательности псевдослучайных чисел, основанном на разложениях полиадических чисел

В. Ю. Матвеев

Матвеев Владимир Юрьевич — кандидат физико-математических наук, Институт экономики, математики и информационных технологий РАНХиГС (г. Москва).
e-mail: salomaa@mail.ru

Аннотация

Цель работы —- построение датчиков псевдослучайных чисел на основе разложений почти полиадических чисел по степеням заданного числа. Полиадическим числом принято называть ряд вида $\sum_{n=0}^{\infty} a_n n!$, где $0 \leqslant a_n \leqslant n$, a_n — целое число. Ряды подобного вида, сходящиеся во всех полях p–адических чисел, кроме конечного их числа, имеющие рациональные коэффициенты, называются почти полиадическими числами.

Рассмотрим функциональные ряды вида $\sum_{n=0}^{\infty} (\lambda)_n z^n$, где $(\lambda)_0 = 1$, $(\lambda)_n = \lambda(\lambda+1)\dots(\lambda+n-1)$, т.е. $(\lambda)_n$ – символ Похгаммера, а λ – рациональное число. Эти ряды, отличные от многочленов, имеют нулевой радиус сходимости в поле комплексных чисел, однако они имеют радиусы сходимости, большие 1 в любом поле p – адических чисел, кроме конечного числа полей p – адических чисел, тех, в которых p входит в знаменатель несократимой дроби λ.

Будем считать, что $\lambda_i = \frac{a_i}{b_i}$, $i = 1, \dots, m$, где a_i, b_i – натуральные числа, Н.О.Д. $(a_i, b_i) = 1$, $i = 1, \dots, m$ и $\lambda_i - \lambda_j \notin \mathbb{Z}$ при $i \neq j$. Можно доказать, что при этих условиях ряды $\sum_{n=0}^{\infty} (\lambda_i)_n (b_i)^n Z^n$, $i = 1, \dots, m$ алгебраически независимы над полем рациональных функций от z [1].

Из этого следует бесконечная алгебраическая независимость полиадических чисел $\sum_{n=0}^{\infty} (\lambda_i)_n (b_i)^n$, $i = 1, \dots, m$ [2].

Можно высказать предположение о том, что цифры разложений частичных сумм $\sum_{n=0}^{N} (\lambda_i)_n (b_i)^n$, $i = 1, \dots, m$ рассматриваемых рядов обладают неплохими статистическими свойствами. В статье описаны результаты проведённых экспериментов.

Ключевые слова: почти полиадические числа, псевдослучайные числа.

Библиография: 15 названий.

Для цитирования:
Матвеев, В. Ю. О подходе к построению последовательности псевдослучайных чисел, основанном на разложениях полиадических чисел // Чебышевский сборник, 2025, т. 26, вып. 4, с. 454–460.

CHEBYSHEVSKII SBORNIK
Vol. 26. No. 4.

UDC: 511.36 DOI: 10.22405/2226-8383-2025-26-4-454-460

An approach to constructing a sequence of pseudorandom numbers based on decompositions of polyadic numbers

V. Y. Matveev

Matveev Vladimir Yur'evich — candidate of physical and mathematical sciences, Institute of Economics, Mathematics and IT of RANEPA (Moscow).
e-mail: salomaa@mail.ru

Abstract

The aim of the work is to construct pseudorandom number generators based on expansions of almost polyadic numbers in powers of a given number. A polyadic number is usually called a series of the form $\sum_{n=0}^{\infty} a_n n!$, where $0 \leqslant a_n \leqslant n$, a_n is an integer. Series of this type, converging in all fields of p–adic numbers, except for a finite number of them, having rational coefficients, are called almost polyadic numbers.

We shall assume that $\lambda_i = \frac{a_i}{b_i}$, $i = 1, \ldots, m$, where a_i, b_i are positive integers, N.O.D. $(a_i, b_i) = 1$, $i = 1, \ldots, m$ and $\lambda_i - \lambda_j \notin \mathbb{Z}$ for $i \neq j$. It can be shown that under these conditions the series $\sum_{n=0}^{\infty} (\lambda_i)_n (b_i)^n Z^n$, $i = 1, \ldots, m$ are algebraically independent over the field of rational functions of z [1].

This implies the infinite algebraic independence of polyadic numbers $\sum_{n=0}^{\infty} (\lambda_i)_n (b_i)^n$, $i = 1, \ldots, m$ [2].

It can be assumed that the expansion digits of the partial sums $\sum_{n=0}^{N} (\lambda_i)_n (b_i)^n$, $i = 1, \ldots, m$ of the series under consideration have good statistical properties. The article describes the results of the experiments conducted.

Keywords: almost polyadic numbers, pseudorandom numbers.

Bibliography: 15 titles.

For citation:
Matveev, V. Yu. 2025, "An approach to constructing a sequence of pseudorandom numbers based on decompositions of polyadic numbers" , *Chebyshevskii sbornik*, vol. 26, no. 4, pp. 454–460.

1. Основной результат

Рассмотрим функциональные ряды вида $\sum_{n=0}^{\infty} (\lambda)_n z^n$, где $(\lambda)_0 = 1$, $(\lambda)_n = \lambda(\lambda+1)\ldots(\lambda+n-1)$, т.е. $(\lambda)_n$ – символ Похгаммера, а λ – рациональное число. Эти ряды, отличные от многочленов, имеют нулевой радиус сходимости в поле комплексных чисел, однако они имеют радиусы сходимости, большие 1 в любом поле p – адических чисел, кроме конечного числа полей p – адических чисел, тех, в которых p входит в знаменатель несократимой дроби λ.

Будем считать, что $\lambda_i = \frac{a_i}{b_i}$, $i = 1, \ldots, m$, где a_i, b_i – натуральные числа, Н.О.Д. $(a_i, b_i) = 1$, $i = 1, \ldots, m$ и $\lambda_i - \lambda_j \notin \mathbb{Z}$ при $i \neq j$. Можно доказать, что при этих условиях ряды $\sum_{n=0}^{\infty} (\lambda_i)_n (b_i)^n z^n$, $i = 1, \ldots, m$. алгебраически независимы над полем рациональных функций от z [1].

Из этого следует бесконечная алгебраическая независимость полиадических чисел $\sum_{n=0}^{\infty} (\lambda_i)_n (b_i)^n z^n$, $i = 1, \ldots, m$ [2].

Термин «бесконечная алгебраическая независимость» требует пояснения. Совокупности значений, принимаемых этими рядами в полях p – адических чисел, можно рассматривать, как бесконечномерные векторы. Операции сложения и умножения этих векторов определяются покоординатно. Это позволяет определить значение многочлена с целыми коэффициентами от таких векторов. Совокупность таких векторов называется бесконечно алгебраически независимой, если для любого многочлена с целыми коэффициентами, отличного от нулевого многочлена, существует бесконечное множество простых чисел p таких, что при подстановке в этот многочлен значений рассматриваемых рядов в поле p – адических чисел получается ненулевое p – адическое число [1]–[13]. Отметим, что из бесконечной трансцендентности не следует хотя бы иррациональность суммы рассматриваемого ряда в конкретном поле p – адических чисел.

Тем не менее, можно высказать предположение о том, что цифры разложений частичных сумм $\sum_{n=0}^{N}(\lambda_i)_n(b_i)^n z^n$, $i=1,\dots,m$ рассматриваемых рядов обладают неплохими статистическими свойствами. В статье описаны результаты проведённых экспериментов.

Отметим вначале, что

$$\alpha_i=\sum_{n=1}^{N}(\lambda_i)_n(b_i)^n=\sum_{n=1}^{N}a_i(a_i+b_i)\dots(a_i+(n-1)\,b_i),i=1,\dots,m,$$

что позволяет легко вычислять каждое следующее слагаемое в этой сумме. Действительно, для каждого $i=1,\dots,m$ положим

$$\begin{gathered}C_{0,i}=a_i,C_{n,i}=C_{n-1,i}+b_i,n=1,2,\dots,N,\\A_{0,i}=a_i,A_{n+1,i}=A_{n,i}C_{n,i},n=0,1,\dots,N-1,\\S_{0,i}=a_i,S_{n+1,i}=S_{n,i}+A_{n+1,i},n=0,1,\dots,N-1.\end{gathered}\tag{1.1}$$

Выбирать целые числа a_i, b_i можно почти произвольным образом, лишь бы только выполнялись условия: $\lambda_i=\frac{a_i}{b_i}$, $i=1,\dots,m$, где a_i, b_i–натуральные числа, Н.О.Д. $(a_i,b_i)=1$, $i=1,\dots,m$ и $\lambda_i-\lambda_j\notin Z$ при $i\neq j$. Выбор чисел m, N зависит от потребностей задачи, для изучения которой требуются псевдослучайные числа.

В качестве примера рассмотрим $m=3$, $N=10000$. Числа $a_1=1$, $b_1=6$, $a_2=7$, $b_2=9$, $a_3=9$, $b_3=10$. Получены 3 числа, имеющие, соответственно, 45660 десятичных и 151676 двоичных знаков. Каждое из этих чисел было подвергнуто проверке с помощью тестов NIST. В приведенных ниже таблицах в правом столбце стоят дроби вида p/q, где q–количество выборок двоичных последовательностей, p – минимальное значение проходимости для каждого статистического теста, за исключением теста на случайное отклонение (вариант). Минимальное значение проходимости для теста на случайное отклонение (вариант) не определено. При проведении тестов размер выборки был задан приблизительно равным 15167 двоичным числам, количество выборок равным 10.[15]

Выбраны наихудшие результаты прохождения тестов.

Наименование в пакете NIST	$a_1 = 1,\ b_1 = 6$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	9/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	10/10
RandomExcursions	– – – – – –
RandomExcursionsVariant	– – – – – –
Serial	10/10
LinearComplexity	9/10

Наименование в пакете NIST	$a_2 = 7,\ b_2 = 9$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	9/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	8/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	8/10
RandomExcursions	– – – – – –
RandomExcursionsVariant	– – – – – –
Serial	10/10
LinearComplexity	10/10

Наименование в пакете NIST	$a_3 = 9,\ b_3 = 10$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	9/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	8/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	9/10
RandomExcursions	– – – – – –
RandomExcursionsVariant	– – – – – –
Serial	9/10
LinearComplexity	10/10

Для проверки совокупного качества полученных последовательностей цифр все эти три последовательности были совмещены в одну (просто поставлены одна за другой) и снова подвергнуты проверке с помощью тестов NIST.

Наименование в пакете NIST	$a_1 = 1,\ b_1 = 6;\ a_2 = 7,\ b_2 = 9;\ a_3 = 9,\ b_3 = 10$
Frequency	10/10
BlockFrequency	10/10
CumulativeSums	10/10
Runs	10/10
LongestRun	10/10
Rank	10/10
FFT	10/10
NonOverlappingTemplate	9/10
OverlappingTemplate	10/10
Universal	10/10
ApproximateEntropy	10/10
RandomExcursions	−−−−−−
RandomExcursionsVariant	−−−−−−
Serial	10/10
LinearComplexity	10/10

2. Заключение

Отметим что специально выбраны наихудшие из результатов испытаний и даже они оказались весьма хорошими. Кроме приведённых выше примеров, были проведены числовые эксперименты с различными m,N и они также дали хорошие результаты.

Планируется расширить класс рассматриваемых объектов и получить новые источники хороших псевдослучайных чисел.[14][15].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Матвеев В. Ю. Бесконечная алгебраическая независимость некоторых почти полиадических чисел. // Чебышевский сборник. 2024;25(3):365–372.

2. Chirskii V. G. Product formula, global relations and polyadic integers. // Russian Journal of Mathematical Physics, 2019, том 26, №3, с. 286–305.

3. Chirskii V. G. Arithmetic properties of generalized hypergeometric F series // Russ. J. Math. Phys., 2020, v.27, no.2, pp.175–184.

4. Чирский В. Г. Об арифметических свойствах обобщенных гипергеометрических рядов с иррациональными параметрами // Известия РАН, серия математическая., 2014, т.78, -№6, с.193–210.

5. Чирский В. Г. Полиадические числа Лиувилля // Чебышевский сборник., 2021, т. 22, вып.3.-е., с.245–255.

6. Чирский В. Г. Арифметические свойства значений обобщенных гипергеометрических рядов с полиадическими трансцендентными параметрами // Доклады Академии наук, сер. матем.информ, проц, управл., 2022, т.506, с.95–107.

7. Чирский В. Г. Трансцендентность p–адических значений обобщенных гипергеометрических рядов с трансцендентными полиадическими параметрами // Доклады Академии наук, сер. матем.информ, проц, управл., 2023, т.510, с.29–32.

8. Чирский В. Г. Трансцендентность некоторых 2-адических чисел // Чебышевский сборник., 2023, т. 24, вып.5, с.194 – 200.

9. Юденкова Е. Ю. Бесконечная линейная и алгебраическая независимость значений F–рядов в полиадических лиувиллевых точках // Чебышевский сборник., 2021, т. 22, вып.2.- е. с.334–346.

10. Матвеев В. Ю. Свойства элементов прямых произведений полей // Чебышевский сборник.- 2019.- т.20.- вып. 2, с. 383 – 390.

11. Крупицын Е. С. Арифметические свойства рядов некоторых классов// Чебышевский сборник., 2019, т. 20, вып. 2, с. 374 – 382.

12. Чирский В. Г. Бесконечная алгебраическая независимость полиадических рядов с периодическими коэффициентами // Доклады Российской академии наук. Математика, информатика, процессы управления, издательство Российская академия наук (Москва), 2024, том 519, с. 16–19

13. Чирский В. Г. Трансцендентность p–адических значений обобщённых гипергеометрических рядов с трансцендентными полиадическими параметрами // Доклады. Российской академии наук. Математика, информатика, процессы управления, издательство Российская академия наук (Москва), 2023, том 510, с. 29–32.

14. Кнут Д. Э. Искусство программирования. Том 2. Получисленные алгоритмы // Москва, Вильямс, 2001, т.2, -832 с. - ISBN 5-8459-0081-6.

15. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // https://doi.org/10.6028/NIST.SP.800-22r1a

REFERENCES

1. Matveev V.Yu. 2024, “Infinite algebraic independence of some almost polyadic numbers”, *Chebyshevskii Sbornik* 25(3) pp. 365–372.

2. Chirskii V.G. 2019, “Product formula global relations and polyadic integers”, *Russian Journal of Mathematical Physics* 26(3) pp. 286–305.

3. Chirskii V.G. 2020, “Arithmetic properties of generalized hypergeometric F-series”, *Russian Journal of Mathematical Physics* 27(2) pp. 175–184.

4. Chirskii V.G. 2014, “On arithmetic properties of generalized hypergeometric series with irrational parameters”, *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya* 78(6) pp. 193–210.

5. Chirskii V.G. 2021, “Polyadic Liouville numbers”, *Chebyshevskii Sbornik* 22(3) pp. 245–255.

6. Chirskii V.G. 2022, “Arithmetic properties of the values of generalized hypergeometric series with polyadic transcendental parameters”, *Doklady Akademii Nauk* 506 pp. 95–107.

7. Chirskii V.G. 2023, “Transcendence of p-adic values of generalized hypergeometric series with transcendental polyadic parameters”, *Doklady Akademii Nauk* 510 pp. 29–32.

8. Chirskii V.G. 2023, “Transcendence of some 2-adic numbers”, *Chebyshevskii Sbornik* 24(5) pp. 194–200.

9. Yudenkova E.Yu. 2021, “Infinite linear and algebraic independence of the values of F-series at polyadic Liouville points”, *Chebyshevskii Sbornik* 22(2) pp. 334–346.

10. Matveev V.Yu. 2019, “Properties of elements of direct products of fields”, *Chebyshevskii Sbornik* 20(2) pp. 383–390.

11. Krupitsyn E.S. 2019, “Arithmetic properties of series of some classes”, *Chebyshevskii Sbornik* 20(2) pp. 374–382.

12. Chirskii V.G. 2024, “Infinite algebraic independence of polyadic series with periodic coefficients”, *Doklady Rossiiskoi Akademii Nauk. Matematika Informatika Protsessy Upravleniya* 519 pp. 16–19.

13. Chirskii V.G. 2023, “Transcendence of p-adic values of generalized hypergeometric series with transcendental polyadic parameters”, *Doklady Rossiiskoi Akademii Nauk. Matematika Informatika Protsessy Upravleniya* 510 pp. 29–32.

14. Knuth D.E. 2001, *The Art of Computer Programming. Volume 2: Seminumerical Algorithms.* Moscow: Williams. 832 p. ISBN 5-8459-0081-6.

15. National Institute of Standards and Technology. 2010, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* NIST Special Publication 800-22Rev1a. Available at: https://doi.org/10.6028/NIST.SP.800-22r1a

Получено: 26.06.2025
Принято в печать: 17.10.2025