УДК 681:51

Глазунов Н.М., д-р .физ.-мат. наук
Кравчук И.В.

КОМПЬЮТЕРНАЯ СИСТЕМА ДЛЯ ИССЛЕДОВАНИЯ ЗАДАЧ РАСПРЕДЕЛЕНИЯ ЗНАЧЕНИЙ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Национальный авиационный университет

Описано применение компьютерной системы для исследования распределения значений числовых последовательностей, а также программа дальнейших экспериментов и проект развития системы

Постановка задачи

Задача исследования распределения значений числовых последовательностей является актуальной как в теоретических, так и в прикладных исследованиях [1,2].

Первым из авторов разработан метод оценки плотностей распределения некоторых числовых последовательностей, а также, на основе этого метода, система программирования для исследования распределения числовых последовательностей и их плотностей [3,4]. Метод и система программирования были им применены для экспериментального исследования распределения значений числовых последовательностей, а также для исследования существующих и гипотетических функций плотности распределения последовательностей в ряде теоретических и прикладных задач [3,4], в частности, для арифметического моделирования случайных процессов.

В работе приведены исследуемая задача, метод её исследования, структура ранее разработанной компьютерной системы, результаты применения системы для исследования распределения значений сумм Клостермана, программа дальнейших экспериментов и направления развития разработанной компьютерной системы.

Суммы Клостермана и проблема оценки их плотностей распределения

Напомним, по рекомендации рецензента, понятие накрытия. Проведем это на примере, входящем в курс теории функций комплексного переменного некоторых технических университетов. Функция корень n-ой степени $w=\sqrt[n]{z}$ из комплексного числа z определяет n-листное накрытие комплексной плоскости, которое является n-листной римановой поверхностью. Суммы Клостермана связаны с расширениями и накрытиями Артина-Шрайера над конечными полями. Такая терминология на русском языке была введена впервые, по видимому, в классической книге [5].

Рассмотрим

$$y^p - y = cx + d/x, \qquad (1)$$

$c, d \in Z, c, d$ не сравнимы с $0 (\mathrm{mod}\, p)$, накрытие Артина-Шрайера над полем $\mathrm{F}_{p^r} (r > 1)$ – конечным расширением поля F_p. Пусть

$$f(t) = t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n, \qquad (2)$$

многочлен из $F_{p^r}[t]$ с $a_n \neq 0$ в F_p.

В некотором конечном расширении k поля F_p имеет место разложение

$$f(t) = (t - \alpha_1)\ldots(t - \alpha_n).$$

Положим

$$l(f) = c(\alpha_1 + \ldots + \alpha_n) + d(1/\alpha_1 + \ldots + 1/\alpha_n),$$

где $\alpha_1, \ldots, \alpha_n$ – корни (2).

Для многочленов вида (2) имеет место

$$l(f_1 f_2) = l(f_1) + l(f_2). \qquad (3)$$

Пусть $T_r F_{p^r} \to F_p$:

$$T_\gamma(l(f_1 f_2)) = T_\gamma(l(f_1)) + T_\gamma(l(f_2)).$$

Для заданного многочлена вида (2) определим характер

$$\chi_\nu(f) = e^{2\pi i \nu Tr(l(f))/p},$$

где ν – одно из чисел множества 0,1,2,..., p-1, $\chi(a) = 0$ если a_n=0 в F_p.

Легко проверить, что $\chi(f_1 f_2) = \chi(f_1)\chi(f_2)$.

Для накрытия вида (1) над F_{p^r} L – функцию определяют равенств

$$L(z,\chi) = \prod_{m=1}^{\infty} \prod_{p(t)} \frac{1}{(1-\chi(p(t))z^m)}, \quad (4)$$

где внутреннее произведение распространяется на все неприводимые в $\mathrm{F}_{p^r}[t]$ многочлены со старшим коэффициентом 1, $\nu \geq 1$. При $\nu = 0$ функция

$$L(z,\chi_0) = (1-p^\gamma z)^{-1}.$$

Положим

$$T_r(\nu;c,d) = \sum_{\xi} e^{2\pi i \nu \frac{Tr(c\xi + d/\xi)}{p}},$$

$\nu = 0,1,2,..., p-1$, ξ пробегает элементы мульти-пликативной группы поля F_{p^r},

$T_p(c,d) = \sum_{x=1}^{p-1} e^{2\pi i \frac{cx+\frac{d}{x}}{p}}$ (сумма Клостермана).

Замечание 1. $T_1(\nu;c,d) = T_p(c,d)$ при $\nu = 1,2,..., p-1$.

Теорема 2. Произведение (4) сходится при $|z| < 1/p^r$. Функция (4) является многочленом второй степени и имеет вид

$$L(z,\chi_\nu) = 1 + T_\gamma(\nu,c,d)z + p^\gamma z^2. \quad (5)$$

Доказательство (следуем А.Г. Постникову, который рассмотрел случай рациональных тригонометрических сумм с простым знаменателем [5]).

Лемма 3. $\sum_{\xi} e^{2\pi i \nu \frac{Tr(\xi)}{p}} = \begin{cases} 0, \nu \neq 0; \\ p^r, \nu = 0. \end{cases}$

где ξ пробегает элементы поля F_{p^r}.

Лемма 4. В условиях теоремы произведение в правой части (4) сходится и имеет место

$$\prod_{m=1}^{\infty} \prod_{p(t)} \frac{1}{(1-\chi(p(t))z^m)} = 1 + \sum_{m=1}^{\infty} \left(\sum \chi(q(t))\right) z^m$$

где внутренняя сумма распространяется на все многочлены из $\mathrm{F}_{p^r}[t]$ степени m со старшим коэффициентом 1.

Доказательство следует из теоремы об однозначности разложения на неприводимые множители в кольце $\mathrm{F}_{p^r}[t]$

Нетрудно видеть, что

$$\sum_{\deg q(x)=1} \chi(q(t)) = \sum_{\xi} e^{2\pi i \nu \frac{Tr(c\xi + d/\xi)}{p}},$$

где ξ пробегает мультипликативную группу поля F_{p^r}.

Лемма 5. Функция (4) является многочленом второй степени вида (5), $\nu = 1,2,..., p-1$.

Теорема 6. Корни произведения (7) имеют абсолютную величину, равную $1/\sqrt{p}$.

Доказательство. Разложим L_p в поле комплексных чисел $\boldsymbol{C}$:

$$L_p = (1-\omega_1 z)(1-\omega_2 z).$$

Тогда аналогично [5] доказывается, что если $W_p(z) = \prod_{\tau=1}^{2(p-1)} (1-\omega_\tau z)$, то

$$W_{p^r}(z) = \prod_{\tau=1}^{2(p-1)} (1-\omega_\tau^r z).$$

Обозначим через $\#T(F_{p^r})$ число решений уравнения $Tr(c\xi + d/\xi) = 0$ относительно ξ в поле F_{p^r}. Имеет место равенство

$$\left| \sum_{\tau=1}^{2(p-1)} \omega_\tau^r \right| = \left| p\#T(F_{p^r}) - p^r - 1 \right|$$

Для его доказательства достаточно сравнить в тождестве

$$\prod_{\tau=1}^{2(p-1)} (1-\omega_\tau^r z) = \prod_{\nu=1}^{p-1} L_{p^r}(\nu),$$

коэффициенты при z в первой степени и показать, что

$$\left|\sum_{\tau=1}^{2(p-1)} \omega_\tau^r\right| = \left|\sum_{\nu=1}^{p-1}\sum_{\xi} e^{2\pi i\nu\frac{Tr(c\xi+d/\xi)}{p}}\right| =$$

$$\left|\sum_{\nu=0}^{p-1}\sum_{\xi} e^{2\pi i\nu\frac{Tr(c\xi+d/\xi)}{p}} - p^r - 1\right| =$$

$$= \left|p\#T(F_{p^r}) - p^r - 1\right|$$

ξ пробегает F_{p^r}. Из леммы 8 [5] следует, что $\#X(F_{p^r}) = p\#T(F_{p^r})$. Теперь разлагая $\ln W_{pr}(z)$ в ряд Тэйлора, получаем

$$\ln W_{p^r}(z) = -\sum_{\tau=1}^{2(p-1)} \ln\frac{1}{1-\omega_\tau z} =$$

$$= \sum_{m=1}^{\infty}\frac{1}{m}\left(\sum_{\tau=1}^{2(p-1)}\omega_\tau^m\right)z^m$$

Однако

$$\left|\sum_{m=1}^{\infty}\frac{1}{m}\left(\sum_{\tau=1}^{2(p-1)}\omega_\tau^m\right)z^m\right| \le$$

$$\le \sum_{m=1}^{\infty}\frac{1}{m}\left|p\#T(F_{p^r}) - p^m\right|^{|z^m|} \le$$

$$\le 2(p-1)\sum_{m=1}^{\infty}\left(\frac{1}{m}p^{m/2}\right)^{|z^m|}$$

Следовательно, ряд

$\ln W_{p^r}(z)$ сходится при $|z| < 1/\sqrt{p}$

Применяя теорему о круге сходимости степенного ряда к $\ln W_{p^r}(z)$ и учитывая, что $\prod_{\tau=1}^{2(p-1)}|\omega_\tau| = p^{p-1}$, получаем

$$|\omega_\tau| = \sqrt{p}$$

$$\tau = 1,2,...,2(p-1)$$

Следствие 7.

$T_p(c,d) = 2\sqrt{p}\cos\theta(c,d)$.

Результаты компьютерных исследований

В [3] изложены (см. также раздел 3 ниже) результаты вычисления углов θ_p сумм Клостермана на интервале $[0,\pi]$ в следующих двух случаях:

А) доказанный Кацем [6] и Адольфсоном [7] случай распределения углов сумм Клостермана

$$T_p(c,d) = \sum_{x=1}^{p-1} e^{2\pi i\frac{\left(cx+\frac{d}{x}\right)}{p}},$$

когда $c,d,\ cd$ не делится на p, независимо пробегают F_p, а p стремится к бесконечности;

Б) проверка гипотезы для суммы

$$T_p = \sum_{x=1}^{p-1} e^{2\pi i\frac{\left(cx+\frac{d}{x}\right)}{p}},$$

c=d=1, на выборке из 1600 последовательных простых, когда сумма фиксирована (фиксированы параметры c и d).

В [3], а также ниже, проведено сопоставление доказанного случая А) с результатами вычислений случая Б).

Методика вычислений и их обработка.

В процессе счета для каждого простого p вычислялись значения T_p, $\cos\theta_p$, θ_p. Приведем таблицу примеров больших и малых по модулю значений $\cos\theta_p$ сумм Клостермана T_p для различных простых p.

Таблица 1. Абсолютные значения $\cos\theta_p$ *(c,d)*

Большие значения		**Малые значения**	
p	$\lvert\cos\theta_p\rvert$	p	$\lvert\cos\theta_p\rvert$
2	0,35355	2	0,35355
7	0,38721	41	0,31430
29	0,47823	97	0,10634
103	0,52564	383	0,08503
1549	0,66391	487	0,05637
3041	0,75232	709	0,04543
5059	0,78164	1613	0,03436
7537	0,85773	2161	0,02577
10181	0,95269	3719	0,01499
13171	0,96537	10889	0,00492

Интервал $[0,\ \pi]$ разбиваем на 20 подинтервалов $U_i = [\frac{(i-1)\pi}{20}, \frac{i\pi}{20}]$,

i= 1,2....20, i – номер интервала U_i, $\nu(U_i)$ – количество углов θ_j,

(где j: $1 \le j \le n$, есть номер последовательного простого) попавших в интервал U_i, $h(U_i)$ - гипотетическое количество углов θ_j, содержащихся в интервале U_i

для данной выборки при $\sin^2 t$ распределении, $P_i = \frac{2}{\pi}\int \sin^2 t dt$, $h(U_i) = \|np_i\|$, где $\|\alpha\|$ ближайшее целое к α, n – число элементов в выборке.

Случай А. Вычисления и теория показывают, что распределения значений углов $\theta_p(c,d)$ сумм

$$T_p(c,d) = \sum_{x=1}^{p-1} e^{2\pi i\left(\frac{cx+\frac{d}{x}}{p}\right)},$$ по интервалам

$$U_i = [\frac{(i-1)\pi}{20}, \frac{i\pi}{20}],\ i = 1,2,\ldots 20,$$ при

c=const, $1 \le d \le p$-1 одинаково при различных $1 \le c \le p$-1. Ввиду этого далее приводятся экспериментальные данные распределения углов сумм T_p(c,d) при c=const, $1 \le d \le p$-1.

Например, для p=1597, c=890, $1 \le d \le p$-1 результаты вычислений суммируются в таблицу 2, обозначения в которой выше описаны.

Таблица 2. Распределение улов $\theta_p(c,d)$, p=1597, c=890, $1 \le d \le$ p-1.

i	$\nu(U_i)$	$h(U_i)$	i	$\nu(U_i)$	$h(U_i)$
1	*0*	*1*	*11*	*154*	*158*
2	*6*	*9*	*12*	*158*	*151*
3	*29*	*24*	*13*	*141*	*136*
4	*51*	*44*	*14*	*109*	*116*
5	*65*	*67*	*15*	*99*	*92*
6	*90*	*92*	*16*	*70*	*67*
7	*111*	*116*	*17*	*44*	*44*
8	*134*	*136*	*18*	*18*	*24*
9	*154*	*151*	*19*	*7*	*9*
10	*153*	*158*	*20*	*3*	*1*
Всего	*793*			*803*	

Подсчитаем теперь по χ^2- критерию Пирсона вероятность отвергнуть гипотезу о $\sin^2 t$ распределении, используя данные таблицы. Так как в каждый интервал должно попадать не менее 10 значений, объединяем интервалы U_1, U_2 и U_3 и интервалы U_{19} и U_{20}.

Утверждение 8. В случае А для таблицы 2.2 с 16 степенями свободы χ^2 =7,52.

Случай Б. Результаты вычислений на выборке из 1600 последовательных простых от 2 до 13499 приведены в таблице 3.

Таблица 3. Распределение углов для 1600 последовательных простых от 2 до 13499

i	$\nu(U_i)$	$h(U_i)$	i	$\nu(U_i)$	$h(U_i)$
1	*0*	*1*	*11*	*164*	*159*
2	*7*	*9*	*12*	*141*	*151*
3	*25*	*24*	*13*	*150*	*136*
4	*41*	*44*	*14*	*128*	*116*
5	*66*	*68*	*15*	*106*	*92*
6	*98*	*92*	*15*	*67*	*68*
7	*99*	*116*	*17*	*40*	*44*
8	*132*	*136*	*18*	*25*	*24*
9	*152*	*151*	*19*	*2*	*9*
10	*156*	*159*	*20*	*1*	*1*
Всего	*776*			*824*	

Обработка результатов вычислений по χ^2 критерию Пирсона аналогична случаю А). Так как в каждый интервал должно попадать не менее 10 значений, объединяем интервалы U_1, U_2 и U_3 и интервалы U_{18}, U_{19} и U_{20}.

Утверждение 9. В случае Б) с 15 степенями свободы

$$\chi^2 = 10{,}1806.$$

Сопоставление вычисленного значения χ^2 с таблицами для χ^2- распределения дает для случая Б): С 5% процентным уровнем значимости по χ^2 критерию Пирсона гипотеза о равнораспределенности углов θ_p на интервале $[0,\pi]$ с функцией плотности $\frac{2}{\pi}\sin^2 t$ верна.

Какие еще задачи необходимо исследовать? Во первых, продолжить вычисления значений сумм Клостермана (Б) для последующих простых с целью получения дополнительных результатов о распределении значений углов сумм Клостермана и их гипотетической плотности распределения.

Во – вторых, провести дополнительные вычисления на слоях при фиксированных *c* или *d* и исследования распределения значений углов сумм Клостермана в случае (А) в конкретном слое, что требуется в некоторых прикладных задачах. И, в – третьих, для решения этих задач необходимо развить пакет ТЧАИ, интегрировать реализованные в нем методы,

и сам пакет, с новыми компьютерными системами.

Компьютерные средства исследования распределения числовых последовательностей

Описанные в предыдущем разделе вычисления были проведены первым из авторов с применением им же разработанной компьютерной системы (КС) ТЧАИ и различных модификаций этой КС [3]. Состав адаптированной к исследованию распределения числовых последовательностей КС ТЧАИ следующий:

а) подсистема порождения (вычисления) числовых последовательностей;

б) база данных, содержащая массив простых чисел, вычисленные числовые последовательности а также средства обновления и модификации;

в) подсистема статистической обработки результатов вычислений.

Приведем здесь некоторые возможности и характеристики пакета *MATLAB*, ориентируясь, в основном, на *Matlab* 7 [8], которые целесообразно интегрировать с КС ТЧАИ.

MATLAB обладает хорошо развитыми возможностями визуализации двумерных и трехмерных данных. Высокоуровневые графические функции призваны сократить усилия пользователя до минимума, обеспечивая, тем не менее, получение качественных результатов. Интерактивная среда для построения графиков позволяет обойтись без графических функций для визуализации данных. Кроме того, она служит и для оформления результата желаемым образом: размещения поясняющих надписей, задания цвета и стиля линий и поверхностей, словом, для получения изображения, пригодного для включения в отчет или статью. Полный доступ к изменению свойств отображаемых графиков дают низкоуровневые функции, применение которых подразумевает понимание принципов компьютерной графики и владение приемами программирования.

В *MATLAB* реализованы классические численные алгоритмы решения уравнений, задач линейной алгебры, нахождения значений определенных интегралов, аппроксимации, решения систем или отдельных дифференциальных уравнений. Для применения базовых вычислительных возможностей достаточно знания основных численных методов в рамках программы технических вузов. Решение специальных задач, разумеется, невозможно без соответствующей теоретической подготовки.

Простой встроенный язык программирования позволяет легко создавать собственные алгоритмы. Простота языка программирования компенсируется огромным множеством функций *MATLAB* и *Toolbox*. Данное сочетание позволяет достаточно быстро разрабатывать эффективные программы, направленные на решение практически важных задач. *MATLAB* прекрасно интегрируется со многими приложениями и средами программирования. Связь *MATLAB* и *MS Word* обеспечивает возможность написания в редакторе *MS Word* интерактивных документов, так называемых *M*-книг, основанных на специальном шаблоне. Пользователь, работающий с *M*-книгой, может запускать блоки команд *MATLAB* непосредственно из документа *MS Word*, причем результат выполнения команд отображается в *M*-книге. Данное средство прекрасно подходит для создания электронных отчетов и учебных пособий. Надстройка *MS Excel Link*, поставляемая вместе с *MATLAB*, существенно расширяет возможности *MS Excel*, обеспечивая доступ пользователя к функциям *MATLAB* и *Toolbox*. Подготовка данных осуществляется непосредственно в электронных таблицах, а обращение к функциям производится либо из ячеек рабочего листа, либо в модуле, написанном на *Visual Basic (VBA)*. *MATLAB Builder for MS Excel* позволяет реализовывать алгоритмы *MATLAB* в виде *COM*-объектов и использовать их в приложениях на *VBA*. Информация, хранящаяся в базах данных многих популярных форматов, может быть импортирована в *MATLAB*, нужным образом обработана и исследована при помощи функций *MATLAB*, а затем экспортирована в какую-либо другую базу данных. Для обмена данными используются команды языка

запросов *SQL*. Поддерживается, в частности, связь с *Microsoft Access, Microsoft SQL Server, Oracle.* Имеется приложение с графическим интерфейсом, которое облегчает работу пользователей, не знакомых с языком запросов *SQL*.

Символические вычисления в *MATLAB* основаны на библиотеке, являющейся ядром пакета *Maple.* Решение уравнений и систем, интегрирование и дифференцирование, вычисление пределов, разложение в ряд и суммирование рядов, поиск решения дифференциальных уравнений и систем, упрощение выражений – вот далеко не полный перечень возможностей *MATLAB* для проведения аналитических выкладок и расчетов. Поддерживаются вычисления с произвольной точностью. Пользователи, имеющие опыт работы в *Maple,* могут напрямую обращаться ко всем функциям данного пакета (кроме графических) и вызывать процедуры, написанные на встроенном языке *Maple.* Программный интерфейс приложения (*API*) реализует связь среды *MATLAB* с программами, написанными на *C, Fortran* или *Java.* Библиотека программного интерфейса позволяет вызывать имеющиеся модули на *C, Fortran* или *Java* из среды или программ *MATLAB*, обращаться к функциям *MATLAB* из программ на *C* или *Fortran*, осуществлять обмен данными между приложениями *MATLAB* и другими программами. Средства *MATLAB Builder for COM* предназначены для преобразования программ *MATLAB* в *COM*-объекты, доступные в других приложениях.

Для разработки интернет-приложений *MATLAB* создан *MATLAB Web Server*, причем процесс создания приложения достаточно прост – кроме умения программировать в *MATLAB* требуется только знание основ *HTML.*

Однако вычисления исследуемых числовых последовательностей эффективнее проводить на ТЧАИ. В настоящее время авторы работают над интеграцией ТЧАИ и отмеченных выше возможностей *MATLAB*.

Выводы

Описаны методы исследования распределения значений числовых последовательностей. Методы применены для экспериментального исследования распределения значений числовых последовательностей, а также для исследования существующих и гипотетических функций плотности распределения последовательностей в ряде теоретических и прикладных задач

На основе проведенных вычислений описываются программа дальнейших экспериментов и направления развития компьютерной системы поддержки таких вычислений.

Список литературы

1. Kable A. Legendre sums, Soto-Andrade sums and Kloosterman sums // Pacific J. of Math. – 2002. Vol. 206. – 1. – P. 139 – 157.

2. A.B. Nobel, G. Morvai, and S. Kulkarni, *Density estimation from an individual numerical sequence*, IEEE Transactions on Information Theory, vol. 44, pp. 537 – 541, 1998.

3. *Глазунов Н.М.* Методы обоснования арифметических гипотез и компьютерная алгебра // Программирование, №3, 2006.

4. Glazunov N.M. On Validated Numerics, Category Theory and Computer Algebra Framework for Simulation and Computation in Theoretical Physics // Nuclear Instruments & Methods in Physics Research, Section A, vol. 502, Nos. 2–3. P. 654 – 656 (2003).

5. *Постников А.Г.* Эргодические вопросы теории сравнений и теории диофантовых приближений. М.: Наука, 1966. – 112 с.

6. Katz N. M. Gauss Sums, Kloosterman Sums, and Monodromy Groups. - Princeton: Princeton Univ. Press, 1988. – 186 p.

7. *Adolphson A.* On the distribution of angles of Kloosterman sums // Journ. fur die reine und angew. Math. – 1989. – 395. – P. 214 – 220.

8. *Ануфриев И., Смирнов А., Смирнова Е.* // Matlab 7 // С.Пб.: БХВ – Петербург, 2005. – 1104 с.