Чан Тхе Ви. Обоснование типов средств транспортировки нефти с морских месторождений СРВ: автореферат дис. ... кандидата технических наук: 05.08.03 / Чан Тхе Ви;[Место защиты: Нижегородского государственного технического университета].- Астрахань, 2006.- 170 с.

Министерство образования и науки Украины

Одесский национальный университет имени И. И. Мечникова

На правах рукописи

ЧАН ТХЕ ВИНЬ

УДК

ПРИМЕНЕНИЯ СУММ КЛОСТЕРМАНА В КРИПТОГРАФИИ И

КОДИРОВАНИИ

Специальность 01.01.08 – Математическая логика, теория алгоритмов и

дискретная математика

Диссертация на соискание ученой степени

кандидата физико-математических наук

Научный руководитель

Варбанец Павел Дмитриевич

доктор физико-математических наук,

профессор

Одесса – 2015

1

СОДЕРЖАНИЕ

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ 3

ВВЕДЕНИЕ 4

РАЗДЕЛ 1

ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ И ВСПОМОГАТЕЛЬНЫЕ

ФАКТЫ

11

1.1. Специальные тригонометрические суммы 11

1.2. Сумма Клостермана над кольцом целых гауссовых чисел G 18

1.2.1. Обобщенные суммы Клостермана над G 27

1.2.2. Теорема 1.1 (Обобщенное тождество Быковского-ВиноградоваКузнецова) 27

1.2.3. Мультипликативные функции, взвешенные суммами

Клостермана 29

1.3. Билинейные формы 41

1.3.1. Билинейные формы с тригонометрическим многочленом 41

1.3.2. Билинейная форма, ассоциированная с гибридной суммой

Клостермана 43

1.4. Линейные коды 50

1.4.1. Порождение новых кодов из заданных кодов 53

1.4.2. Циклические коды 53

1.4.3. Весовой спектр кода, дуального к двоичному линейному коду 54

1.4.4. Теорема Мак-Вильямс для двоичных линейных кодов 55

1.5. Псевдо-случайные числа 59

2

1.5.1. Общие нелинейные конгруентные генераторы с простым

модулем 66

1.5.2. Инверсный конгруентный генератор с простым модулем 69

1.6. Вывод к разделу 1. 73

РАЗДЕЛ 2

ГЕНЕРАТОРЫ ПСЕВДО–СЛУЧАЙНЫХ ЧИСЕЛ 74

2.1. Линейно – инверсный генератор I типа

74

2.2. Линейно – инверсный генератор с переменым сдвигом II типа

. 88

2.3. Линейно – инверсный генератор над кольцом целых гауссовых

чисел с переменным сдвигом

.

102

2.4. Степенной генератор над кольцом целых гауссовых чисел на

норменной группе 115

2.5. Вывод к разделу 2. 124

РАЗДЕЛ 3

ПРИМЕНЕНИЯ СУММ КЛОСТЕРМАНА В КОДИРОВАНИЯ 125

3.1. Код Клостермана 125

3.2. Весовая функция кода Клостермана 130

3.3. Вывод к разделу 3. 134

ВЫВОДЫ 135

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 137

ПРИЛОЖЕНИЯ 150

3

СПИСОК УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ПСЧ – псевдо-случайные числа

– кольца целых рациональных чисел и чисел Гаусса, соответственно

– классы вычетов в (соответственно, в ) по модулю

– редуцированные классы вычетов в (соответственно, в )

– вес Хэмминга вектора

– дуальный код для

– мультипликативное обратное для по модулю , т.е.

– эквивалентные символы, т.е. означает, что

СЛОУ – система линейных однородных уравнений

ЛКГ – линейный конгруентный генератор

– действительная часть комплексного числа

– мнимая часть комплексного числа

4

ВВЕДЕНИЕ

Актуальность темы. Суммы Клостермана появились в работе

Клостермана в 1926 году и в дальнейшем они стали важным инструментом

аналитической теории чисел для решения многих задач, связанных с

построением асимптотических формул теории чисел, теории модулярных форм

и теории кодирования. За последние десятилетия развитие теории сумм

Клостермана и их обобщений обогатило математическую науку новыми

применениями сумм Клостермана в статистической теории чисел,

конструировании новых циклических кодов, исследовании розпределения

весовой функции специальных циклических кодов, а также в тестировании на

псевдо-случайность последовательностей чисел, которые порождены

конгруентными инверсными генераторами. Генераторы псевдо-случайных

чисел являют собой важную составляющую стохастического моделирования,

например, вычисление интегралов и построение решений краевых задач

математической физики по методу Монте Карло. Случайность является

ключевым инградиентом криптографии. Случайные биты используются не

только для генерации криптографических ключей, но часто они являются

главной частью криптографических алгоритмов.

Как правило, источником случайности является псевдо-случайный

числовой генератор, который представляет собой детерминованый алгоритм,

который порождает последовательность чисел с определенными статическими

свойствами. Мы исследуем только равномерно распределенные

псевдослучайные числа. Как известно, неравномерно распределенные псевдослучайные числа можно получить преобразованием равномерного

распределения до необходимого (см., например, монографии А. Г.

Постникова[134] или Л. Девроя[24]). Среди числовых гненераоров

последовательностей псевдо-случайных чисел (в дальнейшем ПСЧ) самыми

распространенными стали конгруентные генераторы, которые впервые

5

появились в роботе Д. Лемера[63]. Этот генератор, хоть и обеспечивал

равнораспределенность последовательности точек на отрезке [0, 1), но не

гарантировали непредвиденности соответствующей последовательности. В

девяностых годах двадцатого столетия в работах Ейченауэра, Лехна,

Нидеррайтера, Емерих и других было доказано, что нелинейные генераторы

при определенных условиях удовлетворяют требованиям

равнораспределенности и статической независимости последовательностей,

порожденных конгруентными генераторами , где –

целозначная нелинейная функция. Особенно привлекательными и в

достаточной мере исследованы инверсные конгруентные генераторы,

ассоциированные с функцией вида .

И вот почти 30 лет такие генераторы исследуются и обобщаются в теории

псевдо-случайных чисел. Кроме того расширяется область использования

последоательностей ПСЧ в криптографии.

Поскольку в криптографических использованиях ПСЧ функция

(точнее ее параметры) являются секретными, то возникает вопрос можно ли по

отдельным элементам сгенерированной последовательности ПСЧ

регенерировать функцию . В работах Блэкберна, Гомез-Перез, Гутиереза,

Шпарлинского было доказано, что при определенных условиях можно

восстановить функцию , если известны первые (или последние) биты

последовательных чисел последовательности ПСЧ. С целью усложнения

процесса регенерации параметров функции в статьях П. Варбанца и С.

Варбанца[112], [113] изучаются конгруентные рекурсии с переменным сдвигом.

Обоснование этой пооблемы также упирается на оценки тригонометрических

сумм Клостермановского типа. Фундаментальная связь между

последовательностями ПСЧ и тригонометрическими суммами дает неравенсто

Турана-Ердёша-Коксмы, в котором дискрепантная функция данной

последовательности (которая измеряет различие в поведении

последовательности ПСЧ и последовательностью значений реализации

6

последовательности равномерно распределенных и независимых случайных

величин) оценивается с помощью оценок тригонометпических сумм на

элементах последовательности ПСЧ. Суммы Клостермана над конечными

полями позволяют изучать распределение значений весовой функции многих

циклических кодов. Этой проблематике посвящены исследования Kim D. S.[57],

La Guardia G.G.[60], Lachaud G., Wolfmann J.[61], Moisio M.[72], Moisio M.[73],

Wolfmann J.[116].

Все вышесказанное свидетельствует об актуальности исследований

свойств числовых генераторов последовательностей ПСЧ, специальных

циклических кодов и соответствующих тригонометрических сумм, котороым и

посвящена данная дисертационная работа.

Связь работы с научными программами, планами, темами.

Дисертационные исследования проводились на кафедре компьютерной алгебры

и дискретной математики института математики экономики и механики

Одесского национального университета имени И. И. Мечникова как часть

научно-исследовательской темы "Использование тригонометрических сумм в

криптографии" (номер государственной ренистрации 0114U001489, 2014 – 2018

г.г.).

Также дисертационные исследования выполнялись в рамках научноисследовательской темы "Исследования асимптотических задач компьютерной

алгебры и аналитической теории чисел" (номер государственной регистрации

0107U4004622, 2009 – 2013 г.г.).

Цель и задачи исследования. Целью исследования является

использование сумм Клостермановского типа в задачах генерирования

последовательностей псевдо-случайных чисел конгруентными инверсными

генераторами, а также в задачах распределения весовой функции циклического

кода Клостермана.

Объектом исследования являются суммы Клостермана и их обобщения

над кольцами целых рациональных и целых гаусовых чисел,

7

последовательности псевдо-случайных чисел и весовая функция циклического

кода.

Предметом исследования являются свойства конгруентных инверсных

генераторов, их дискрепантные функции и оценки тригонометрических сумм на

последовательностях ПСЧ

Задачами исследования является:

˗ построить асимптотическую формулу для сумматорной функции

произвольной мультипликативной функции, которая взвешена суммой

Клостермана;

˗ обобщить оценку билинейной функции, ассоциированную с сумой

Клостермана нал кольцом целых гаусовых чисел;

˗ исследовать свойства последовательности ПСЧ, которая генерируется

линейно-инверсным генератором I и II типов по модулю степени простого

числа;

˗ найти аналог неравенства Турана-Эрдёша-Коксмы для

последовательностей комплексных ПСЧ;

˗ исследовать распределение значений функции веса Хэмминга для кодов

Клостермана

Методы исследования. В работе используются методы теории

тригонометрических сумм над конечными полями и кольцами, теории чисел,

динамических систем, линейной алгебры.

Научная новизна полученных результатов. В дисертации автором

получены такие новые результаты:

˗ для специального класса мультипликативных функций разработан

метод исследования сумматорной функции для взвешенной суммой

Клостермана мультипликативной функции;

˗ найден аналог асимптотической оценки билинейной функции

ассоциированной с суммами Клостермана;

8

˗ для линейно-инверсных генераторов с переменным множителем

линейной части доказана равнораспределенность и непредсказуемость

порождаемых последовательностей ПСЧ;

˗ дано описание условий, при которых последовательность ПСЧ для

линейно-инверсного генератора имеет максимальный период;

˗ построены нетривиальные оценки дискрепантной функции

последовательности ПСЧ, порожденной линейно-инверсным генератором;

˗ построен аналог степенного генератора ПСЧ над кольцом целых

гаусовых чисел на нормений подгруппе и исследована дискрепантная

функция соответствующей последовательности;

˗ найден аналог неравенств Турана-Эрдёша-Коксмы для

последовательностей комплексных чисел в круге ;

˗ в терминах сумм Клостермана над кольцом целых гаусовых чисел

найдена рекурентная формула для вычисления моментов сумм Клостермана и

исследовано распределение весовой функции кода Клостермана.

Практическое значение полученных результатов. Работа имеет

теоретический характер. Разработаные в дисертационной работе методы могут

использоваться для дальнейшего исследования конгруентных генераторов ПСЧ,

а также циклических кодов, ассоциированных с линейно-инверсной функцией.

Результаты дисертационной работы могут стать математической основой

для разнообразных разработок в сфере информационных технологий.

Конгруентные рекурсии, свойства которых исследуются в диссертации, могут

создавать генераторы ПСЧ, которые используются в криптографии,

моделировании случайных процессов, при проектировании компьюторных

сетей.

Диссертация может быть использована для чтения спецкурсов по теории

кодирования и теории криптографических систем на механико-математических

факультетах университетов.

9

Личный вклад автора. Основные результаты диссертации, которые

выносятся на защиту, получны автором самостоятельно. В работах,

опубликованных в соавторстве, личный вклад соискателя состоит в следующем:

˗ в работе [1] автору принадлежат доказательства лем 5 и 6 и

асимптотическая формула для сумматорной функции ;

˗ в работе [2] научному руководителю принадлежит постановка задачи и

общее руководство;

˗ результат статей [3] принадлежит всем авторам в равной мере;

˗ основные результаты работы [4] принадлежат соискателю;

˗ работа [5] выполнялась соискателем самостоятельно, а его научному

руководителю принадлежит выбор основной рекурсии для пораждающего

генератора.

Апробация результатов диссертации. Результаты диссертации

докладывались и обговаривались на:

˗ международной научной конференции, посвященной 120-летию

Стефана Банаха, г. Львов (сентябрь 2012 г.);

˗ международной математической конференции, посвященной 70-летию

проф. В. Кириченко, г. Николаев ( июль 2012 г.);

˗ международной научной конференции "Компьютерная алгебра и

информационные технологии", г. Одесса (август 2012 г.);

˗ международной алгебраической конференции, посвященной 100-летию

Л. А. Калужнина, г. Киев (июль 2014 г.);

˗ XVI - международной научной конференции имени ак. М. Кравчука, г.

Киев (май 2015 г.);

˗ X - международной алгебраической конференции, посвященной 70-

летию проф. Ю. А. Дрозда, г. Одесса (август 2015 г.);

˗ по теории графов и дискретной математики ( Одесский национальный

университет имени И. И. Мечникова, руководители - д. ф. - м. н., проф. О. О.

Зыков и д. ф. - м. н., проф. П. Д. Варбанец, 2013-2015 г.г.);

10

˗ алгебраическом семинаре Киевского национального университета

имени Тараса Шевченка (Киевский национальный университет имени Тараса

Шевченка).

Список публикаций по теме диссертации с указанием личного вклада

искателя.

По результатам исследований опубликовано 14 научных трудов список

публикации указан в списке использованной литературы [1-9] и [135-139], в том

числе, 5 статей в научных профильных изданиях Украины, 2 статьи в изданиях

иностранных государств, которые включены в международные

научнометрические базы, и 2 - иностранные издания, и 5 тезисов докладов в

сборниках материалов конференций.

Структура диссертационной работы. Диссертация состоит из введения,

3 разделов, выводов, списка использованных источников и двух приложении с

фрагментами программных кодов. Общий объем диссертации составляет 160

страницы, из них 136 страниц текста, 11 страниц приложений, список

использованных источников занимает 13 страниц и включает 134

наименования.

ВЫВОДЫ

ВдиссертациирассматриваютсяприменениясуммКлостерманакольца

целыхрациональныхицелыхгауссовыхчиселвкриптографииикодировании

Приэтомполученыновыерезультатыосвойствахэтихсумм

Доказаночтомультипликативныефункцииопределяемыесвёртной

Дирихлесовполнемультипликативнойфункциейивзвешенныесуммами



Клостерманаимеютсумматорныефункциидлякоторыхасимптотические

формулымогутбытьполученывтерминахдзета–подобныхфункций

ИсследованысуммыКлостермананадкольцомцелыхгауссовыхчисел

доказанакорневаяоценкадлятакихсуммнадкольцомклассоввычетовпо

модулюстепенипростогочислаДлянеполныхсуммКлостермананадкольцом

целыхчиселнайденаоценкасоответствующейбилинейнойформыПостроены

новыелинейноинверсныегенераторыпсевдослучайныхчиселобобщающие

известныеинверсныегенераторыВведеныгенераторыспеременнымсдвигом

чтообеспечиваетсекретностьпараметровэтихгенераторовДискрепантные

функциидляпоследовательностейпсевдо–случайныхчиселотрязка

порожденныхлинейно–инверснымигенераторамиоцениваютсяспомощью

оценоктригонометрическихсуммКлостермановскоготипапричёмэти

последовательностипроходятсериальныйтестнаравномерностьи

статистическуюнезависимостьИсследованновыйгенератор

последовательностикомплексныхчиселспеременнымсдвигомНайдено

представлениеэлементовэтойпоследовательностиввидемногочленовот

номераэлементаиинициальногозначенияпорождающейрекурсии

Соответствующиепоследовательностипроходяттестынапсевдо–

случайностьапотомумогутприменятьсявкриптографииПостроенаналог

степенногогенераторананорменнойподгруппекольцаклассоввычетовпо

модулюстепенипростогорациональногочислаОценка

дискрепансиипоследовательностикомплексныхчиселполученаспомощью

аналоганеравенстваТурана–Эрдёша–Коксмыполученноговдиссертации

ИсследованораспределениезначенийвесаХэммингакодовыхслов

Клостермановскогокоданадкольцомклассоввычетовпомодулю

вкольцецелыхгауссовыхчиселВтерминахсуммКлостермана

ивесовкодовыхсловполученарекурсивнаяформуладлявычисления–ых

моментовсуммКлостермананадкольцомцелыхгауссовыхчисел





КлючевыесловасуммыКлостерманасумматорнаяфункцияпсевдо–

случайныечисларавнораспределенностьнепредсказуемостьдискрепансия

кольцоцелыхгауссовыхчиселлинейно–инверсныйгенераторпсевдо–

случайныхчиселвескодовогословакодКлостермана