ОТЗЫВ

официального оппонента о диссертации Миронкина Владимира Олеговича «Явные формулы для распределений характеристик итераций случайных отображений», представленной на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» (физико-математические науки)

Актуальность и значимость темы. Диссертация В. О. Миронкина посвящена изучению характеристик итераций случайных отображений. В работе рассматриваются итерации равновероятного случайного отображения и композиции независимых равновероятных случайных отображений. Такие модели являются примерами неравновероятных отображений, имеющих широкое применение при решении разнообразных задач информационной безопасности. Свойства равновероятных случайных отображений хорошо изучены, но потребности разработки новых методов защиты информации вызвали необходимость исследования более сложных итерационных моделей. Кроме того, возникающие в таких исследованиях математические задачи представляют и самостоятельный интерес, и их решение позволяет существенно развивать современные вероятностные методы дискретной математики, в частности, теории случайных отображений. Таким образом, тема диссертации является актуальной и значимой.

Краткая характеристика основного содержания диссертации. Работа состоит из введения, двух глав и заключения. Во введении обосновывается актуальность проведенного исследования и дается достаточно подробный обзор литературы по теме диссертации. Кратко описывается содержание работы и приводится информация о практической ценности полученных результатов для решения некоторых задач защиты информации.

В первой главе рассматриваются k-кратные итерации равновероятного случайного отображения конечного множества в себя для любого натурального k. Естественно, что для удобства изложения используется понятие графа отображения (и, соответственно, графа итерации), в котором под вершинами понимаются элементы множества, а дугами служат ориентированные ребра, направленными от вершин к их образам. Найдено распределение вероятностей длины отрезка апериодичности (теоремы 1.1 и 1.2). Вычислены вероятности попадания фиксированного элемента в образ множества (теорема 1.3). Вычислены вероятности попадания фиксированного элемента множества в один из циклов заданной длины графа (теорема 1.4). Найдены также вероятности одновременного попадания двух разных элементов в циклы, длины которых заданы и могут быть разными

(теорема 1.5). Доказана теорема 1.6 о вероятности попадания вершин в слои циклов заданной длины. Один из разделов первой главы посвящен нахождению вероятностей инцидентности фиксированной вершины графа компоненте связности, содержащей другую фиксированную вершину (теоремы 1.7 – 1.9). Там же содержится комментарий об особенностях формирования множества производных ключей с использованием итерационной процедуры в случае, когда граф итерации отображения является связным. В связи с этим доказана теорема 1.10 о вероятности единственности компоненты связности. В конце первой главы выведены вероятности инцидентности вершины множеству прообразов другой вершины (теорема 1.11) и вероятности появления коллизий (теорема 1.12). Здесь же кратко упоминается и прикладное значение этих результатов.

Во второй главе изучаются композиции k независимых равновероятных случайных отображений, где k – любое натуральное число. Целесообразность изучения таких композиций обосновывается получением результатов, полезных для повышения теоретической стойкости итерационных алгоритмов формирования ключей. Для таких композиций решались задачи, аналогичные рассмотренным в первой главе для итераций. Найдена функция распределения длины отрезка апериодичности (теорема 2.1). Вычислены как вероятности попадания вершины графа композиции в один из циклов заданной длины (теорема 2.2), так и вероятности совместного попадания двух разных вершин в циклы (теорема 2.3). Вероятности попадания вершин в слои циклов графа композиции найдены в теореме 2.4. Доказаны утверждения о коллизиях (теорема 2.5), о вероятностях попадания вершин в множество образов (теорема 2.6) и о вероятностях попадания вершин в компоненту связности, содержащую заданную вершину (теорема 2.8). Теорема 2.9 является аналогом теоремы 1.11.

Большинство полученных в диссертации формул являются комбинаторными. Многие из них достаточно удобны для использования. Есть среди них и громоздкие, трудно обозримые и, видимо, требующие значительного объема вычислений в задачах больших размерностей. В этих случаях можно надеяться, что применение современных компьютеров решает эту проблему. Работа содержит много следствий из теорем, в некоторых из которых найдены математические ожидания рассмотренных случайных величин, а также оценки исследуемых вероятностей, выраженные в виде неравенств.

В заключении кратко подводятся итоги проделанной работы и намечаются перспективные направления дальнейших исследований модификаций случайных отображений с учетом возможности их применения при решении задач информационной безопасности.

Научная новизна и практическая значимость результатов исследований. Выносимые на защиту результаты являются новыми. Их использование может быть полезно при разработке и анализе современных итерационных алгоритмов защиты информации, что подтверждается актами о внедрении. Работа написана на хорошем математическом уровне. Достоверность результатов подтверждается приведенными строгими доказательствами, публикацией их в рецензируемых журналах и апробацией на всероссийских конференциях, симпозиумах и семинарах. Подавляющее большинство утверждений нетривиальны и для их доказательства автору потребовались глубокие знания об объекте изучения, используемых методах и изобретательность при их применении.

Текст автореферата соответствует тексту диссертации.

Замечания.

1. Случайное отображение в диссертации обозначено буквой f (Предложение 1.1). Однако определение 1.1 графа отображения G_f и другие определения далее сформулированы, исходя из того, что отображение f детерминировано и такой граф уже не рассматривается, как случайный. Это создает некоторые трудности при чтении, особенно в доказательствах. Было бы лучше, если бы случайное и конкретное отображения обозначались по-разному, как это сделано, например, в известной книге В. Ф. Колчина «Случайные отображения».
2. Некоторые из полученных формул выглядят весьма громоздко и, естественно, возникает вопрос о вычислительной сложности реализующих эти формулы алгоритмов при решении задач большой размерности. Возможно, ответ на этот вопрос прояснил бы целесообразность анализа асимптотического поведения соответствующих вероятностей. В диссертации эти вопросы почти не обсуждаются и данное замечание можно рассматривать как пожелание рассмотреть их в будущем.
3. Теорема 1.3, доказанная в первой главе, во введении почему-то имеет номер 1.4 и такой сдвиг в нумерации допущен и во всех следующих теоремах первой главы.
4. Последние две формулы в разделе 2.4 имеют номера (2.36) и (2.37). При этом две другие формулы в начале раздела 2.5 тоже имеют такие же номера. В связи с этим можно заметить, что есть ссылки на номера формул, расположенных значительно ниже места ссылки. Так, например, в формулировке и в доказательстве теоремы 2.6 имеются ссылки на (2.37), при этом обе формулы с таким номером расположены ниже.

Перечисленные замечания не имеют принципиального значения и не влияют на общую положительную оценку диссертации.

Заключение по диссертации. В диссертации содержится решение ряда актуальных задач теории случайных отображений. Полученные результаты вносят важный вклад в развитие этой теории. Содержание работы соответствует паспорту специальности 05.13.19. Диссертация В.О. Миронкина «Явные формулы для распределений характеристик итераций случайных отображений» соответствует критериям, установленным в Положении о присуждении ученых степеней в Московском государственном университете им. М. В. Ломоносова и ее автор, Миронкин Владимир Олегович, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:

доктор физико-математических наук, профессор,
главный научный сотрудник Института
прикладных математических исследований
Карельского научного центра РАН

Павлов Юрий Леонидович

Контактные данные:
тел. +79217273733, email: pavlov@krc.karelia.ru
Специальность, по которой официальным оппонентом защищена диссертация: 01.01.05 – «Теория вероятностей и математическая статистика».
Адрес места работы: 1850910, г. Петрозаводск, ул. Пушкинская, д. 11, КарНЦ РАН, тел.: +7(9142)781218

Подпись Павлова Ю.Л. заверяю
Ученый секретарь ИПМИ КарНЦ

О. В. Лукашенко