

Информационный листок № 5

КЛЕТОЧНЫЕ АВТОМАТЫ

1. Базров, С. А. Модель клеточного автомата маневрирования транспортного средства в потоке / С. А. Базров, А. С. Алёшкин // International journal of open information technologies. – 2023. – Т. 11, № 4. – С. 14-20. – URL : <https://www.elibrary.ru/item.asp?id=50758095> (дата обращения : 06.12.2023)

Управление городскими транспортными сетями является важной задачей, влияющей на многие аспекты жизни современного города. Для оптимизации транспортных потоков города, для выявления критичных мест и для выработки рекомендаций к управлению транспортной сетью требуется проводить сбор данных о дорожном трафике, а, после формирования гипотезы о возможном улучшении ситуации, требуется проводить моделирование движения транспорта. Одним из подходов к подобной симуляции может быть подход с использованием правил клеточного автомата для симуляции движения отдельного автомобиля. В данной работе рассматривается построение клеточного автомата от его элементарной линейной версии (имеющий наименование «Правило 184»), до расширенной версии, учитывающей маневрирование нескольких участников дорожного движения. В статье описан порядок формирования правил для клеточного автомата моделирования движения автомобиля, с учётом возможного маневрирования в потоке и координации движения нескольких транспортных средств (за счёт возможностей кооперативного перестроения). В качестве базовых правил использованы механизмы контроля безопасной скорости, формирования предпочтительного перестроения и учёт возможных состояний, когда несколько участников взаимно-блокируют движение друг друга. Разработанные правила позволяют спроектировать клеточный автомат для моделирования движения автомобиля с возможностью маневрирования в потоке и координации движения нескольких транспортных средств (за счёт возможностей кооперативного перестроения).

2. Бобков, С. П. Использование вероятностных клеточных автоматов для моделирования течения жидкости / С. П. Бобков, И. А. Астраханцева // Современные наукоемкие технологии. Региональное приложение. – 2022. - № 2 (70). – 47-54. – URL : <https://www.elibrary.ru/item.asp?id=49101014> (дата обращения : 06.12.2023)

В статье представлены результаты применения систем вероятностных клеточных автоматов для моделирования процессов течения сплошной среды под действием давления. Использовалось предположение, что вектор скорости частиц потока состоит из двух компонентов - детерминированного и стохастического. Первый определялся в соответствии с основными положениями механики и законом Ньютона для вязкой среды. Для определения случайного компонента вектора скорости принимался принцип одинаковых шагов. Считалось, что направление данной составляющей скорости определяется случайным выбором из четырех ортогональных. Результаты численных экспериментов с моделью показали, что вид поля скоростей частиц и траекторий их

движения более близки к действительным, по сравнению с моделями плоскопараллельного движения. В то же время, в отличие от классических подходов термодинамики, здесь не использовались сложные построения в виде дифференциальных уравнений с частными производными, что значительно упрощает процесс анализа и компьютерной визуализации потоков.

3. Бобков, С. П. Особенности использования систем клеточных автоматов при моделировании основных процессов переноса / С. П. Бобков, И. А. Астраханцева // Современные наукоемкие технологии. Региональное приложение. – 2023. - № 2 (74). – С. 49-59. – URL : <https://elibrary.ru/item.asp?id=54166939> (дата обращения : 06.12.2023)

Статья посвящена современным подходам к моделированию процессов молекулярного переноса вещества. Рассматриваются трудности, возникающие при использовании классических непрерывных моделей в форме дифференциальных уравнений с частными производными. Отмечается, что избежать возникающих проблем позволяет переход к дискретным моделям. Описывается один из дискретных методов моделирования - использование систем клеточных автоматов. Дается общее описание метода и вопросы его конкретного использования для изучения процессов диффузии. Приводятся примеры моделирования процесса диффузии в неоднородных средах, а также в условиях нелинейности процесса. Показано, что использование систем клеточных автоматов предоставляет широкие возможности для создания эффективных алгоритмов и программ моделирования различных процессов молекулярного переноса. Отмечается, что предложенный подход может быть рекомендован для использования в научных исследованиях и практических разработках.

4. Васильев, Д. И. Нижняя оценка сложности задачи поиска ближайшего соседа на прямой с помощью клеточного автомата с локаторами / Д. И. Васильев, Э. Э. Гасанов // Вестник московского университета. Серия 1: математика. Механика. – 2023. - № 5. – С. 33-39. – URL : <https://www.elibrary.ru/item.asp?id=54669690> (дата обращения : 06.12.2023)

Рассматривается применение модели клеточного автомата с локаторами к задаче поиска ближайшего соседа на прямой. Модель клеточного автомата с локаторами подразумевает возможность каждой ячейке автомата передавать через эфир сигнал на сколь угодно большие расстояния. Ранее было показано, что такая возможность позволяет решать задачу поиска ближайшего соседа за логарифмическое время. В работе получена логарифмическая нижняя оценка для сложности этой задачи.

5. Зарубин, Д. М. Метод обеспечения защиты передаваемых сообщений в системе ADS-B с использованием аппарата клеточных автоматов / Д. М. Зарубин, В. П. Добрица, Е. А. Титенко // Известия ЮФУ. Технические науки. – 2022. - № 5 (229). – С. 17-29. – URL : <https://www.elibrary.ru/item.asp?id=50072300> (дата обращения : 06.12.2023)

Цель исследования - разработка метода кодирования передаваемых ADS-B сообщений между воздушными судами в процессе полета. Открытый формат 1090ES передаваемых данных является критическим в плане проведения различных типов атак, которые могут привести к нарушению безопасности полетов воздушных судов. Работа направлена на применение средств кодирования и декодирования сообщений с закрытым ключом. Методы исследования основаны на применении и развитии потокового шифрования данных с использованием одномерных клеточных автоматов. Они работают в режиме генератора псевдослучайных последовательностей, преобразующих элементарных состояний ячейки одномерного клеточного автомата на основе типовых аппаратно-ориентированных операций. В основу процессов кодирования и декодирования полей данных положена аналитическое выражение, использующее типовые логические операции (дизъюнкция, сумма по модулю два). Это свойство позволяет вести параллельную обработку полей данных сообщения и создавать неповторяющиеся последовательности кодов. Результаты - создан метод обеспечения защиты передаваемых данных, дополнительно кодирующий на передаче и декодирующий на приеме сообщения. Отличительная особенность метода - сохранение формата протокола. Выполнена оценка вычислительной сложности работы клеточного автомата. Метод использует одномерный клеточный автомат, который выполняет кодирование и декодирование целевых полей (координаты, курс и др.) с использованием генератора псевдослучайных чисел. Разработанный метод относится к классу аппаратно-ориентированных методов. Критические для кодирования и декодирования свойства периодичности полей данных и длины ключа устраняются путем выбора начального иррационального значения и организации «потоковой» работы кодировщика. Если кодирующий автомат работает в потоковом режиме, текущее значение зависит от предыстории некоторой глубины, определение длины «автоматического ключа» из ADS-B сообщения будет алгоритмически невозможно в силу потери данных. Линейная сложность метода позволяет выполнять преобразования со скоростью потока передачи данных. Вывод - развитие аппаратно-ориентированных методов шифрования данных позволяет повысить эффективность использования системы ADS-B за счет противодействия различным типам деструктивных акций.

6. Ильичев, В. Ю. Исследование динамики поведения клеточных автоматов / В. Ю. Ильичев, Д. С. Каширин // E-SCIO. – 2023. - № 1 (76). – С. 223-233. – URL : <https://elibrary.ru/item.asp?id=50341741> (дата обращения : 06.12.2023)

В статье рассмотрены понятия, используемые при работе с клеточными автоматами, сферы применения данных структур, а также описаны созданные авторами программы, способные рисовать клеточные автоматы двух типов. Первая программа создаёт клеточный автомат в виде матрицы чисел; вторая программа предназначена для наблюдения за динамикой рисуемого на экране компьютера двумерного клеточного автомата, проявляющего как признаки хаотичного, так и признаки упорядоченного поведения. Делается попытка объяснить данный, не исследованный пока, феномен. Даются рекомендации по дальнейшему развитию данного направления исследований, способному объяснить многие факты окружающего мира.

7. Использование математического аппарата клеточных автоматов для решения задачи мониторинга объектов критической инфраструктуры беспилотными летательными аппаратами / В. В. Чистов, И. В. Захарченко, В. М. Павленко [и др.] // Проблемы региональной энергетики. – 2022. - № 3 (55). – С. 156-167. – URL : <https://www.elibrary.ru/item.asp?id=49345107> (дата обращения : 06.12.2023)

Целью данной работы является повышение оперативности и снижения экономических затрат в процессе мониторинга объектов критической инфраструктуры группой подвижных объектов в различных условиях за счет использования математического аппарата клеточных автоматов. Поставленная цель достигается путем минимизации времени полета беспилотных летательных аппаратов, определения и формального описания процесса мониторинга, определения необходимого количества мониторинговых групп, поддержания уровня информированности об объектах наблюдения. В основу построения формальных моделей положен аппарат клеточных автоматов, который позволяет описать сложные поведенческие модели и реализовать существующие природные механизмы решения подобных задач. Наиболее существенными результатами являются формальное описание пространства решения задачи, свойств взаимодействующих объектов, а также разработанные стратегии поведения клеточного автомата, что позволяет реализовать различные поведенческие модели или стратегии решения задачи, а также повысить оперативность и качество решаемой задачи. Значимость полученных результатов состоит в возможности решения сложной задачи многокритериальной оптимизации по нахождению маршрута передвижения группы беспилотных летательных аппаратов для мониторинга объектов критической инфраструктуры. Решение данной задачи позволит оптимизировать экономические затраты на реализацию мониторинга, повысить оперативность и качество производимого мониторинга, а также повысит охват объектов мониторинга. Таким образом проведенные исследования показали эффективность использования клеточных автоматов для решения задач поиска маршрутов при поиске и мониторинге объектов критической инфраструктуры в различных условиях. Использование предложенного аппарата позволяет так же решать задачи подбора характеристик групп поиска, их численного состава и количества групп поиска для решения различных задач. Так же полученные результаты показали независимость результатов и эффективности работы клеточного автомата от начальных условий. Предложенный подход к реализации клеточных автоматов позволит создать эффективную систему мониторинга за состоянием объектов наблюдения, что позволит минимизировать количество и состав групп мониторинга.

8. Ключарев, П. Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 2 / П. Г. Ключарев // Вопросы кибербезопасности. – 2022. - № 1 (47). – С. 37-48. – URL : <https://elibrary.ru/item.asp?id=47690467> (дата обращения : 06.12.2023)

Цель статьи: аналитический обзор применения клеточных автоматов и их обобщений в криптографии. Метод исследования: анализ научных публикаций по теме статьи. Полученные результаты: в обзорной статье проанализирована литература,

посвященная использованию как классических клеточных автоматов, так и их обобщений для построения криптографических алгоритмов. Статья состоит из двух частей. Первая часть была посвящена классическим клеточным автоматам и основанным на них симметричным криптографическим алгоритмам. В ней кратко обсуждалась история развития теории клеточных автоматов и ее применения в различных научных областях. Был приведен обзор работ ряда авторов, которыми предлагались симметричные криптографические алгоритмы и генераторы псевдослучайных последовательностей, основанные на одномерных клеточных автоматах. Стойкость таких криптоалгоритмов оказалось недостаточной. Далее был дан обзор статей, посвященных использованию двумерных клеточных автоматов для построения симметричных криптоалгоритмов (этот подход давал лучшие результаты). Также были упомянуты многомерные клеточные автоматы. Настоящая вторая часть статьи содержит обзор работ, посвященных использованию обобщенных клеточных автоматов в криптографии - на основе таких автоматов возможно создавать алгоритмы симметричного шифрования и криптографические хэш-функции, обладающие высоким уровнем криптостойкости и высокой производительностью при аппаратной реализации (например, на программируемых логических интегральных схемах), а также предъявляющие достаточно низкие требования к аппаратным ресурсам. Кроме того, уделено внимание интересным связям обобщенных клеточных автоматов, в контексте их использования в криптографии, с теорией расширяющих графов; также уделено внимание вопросам стойкости криптоалгоритмов, основанных на обобщенных клеточных автоматах. Упомянуты работы, посвященные реализации различных криптографических алгоритмов, основанных на обобщенных клеточных автоматах, на программируемых логических интегральных схемах и графических процессорах. Дан обзор асимметричных криптоалгоритмов, основанных на клеточных автоматах. Рассмотрены вопросы о принадлежности некоторых задач на клеточных автоматах и их обобщениях к классу NP-полных задач, а также к некоторым другим классам сложности.

сост. Калашникова Ю.А.