$$\Omega^{m}{}_{[w,h]} = \left(\left[\frac{m}{w}\right] + \left[\frac{m-1}{w}\right] + \cdots + \left[\frac{w+1}{w}\right] + 1 \right) \cdot \bullet \left(\left[\frac{m}{h}\right] + \left[\frac{m-1}{h}\right] + \cdots + \left[\frac{h+1}{h}\right] + 1 \right),$$

где w и h представляют ширину и высоту прямоугольных элементов соответственно. Из этой формулы ясно, что число возможных исходов огромно, и метод библиотеки «OpenCV» устраняет этот недостаток путем введения метода интегрального изображения. Пусть f будет произвольное изображение, тогда g — целостный образ этого изображения. В таком случае значение любого пикселя A(x,y) определяется как:

$$g(x,y) = \sum_{x' \le x, y' \le y} f\left(x', y'\right).$$

Рассчитанный по следующей формуле, он равен:

$$s(x,y) = s(x,y-1) + f(x,y),$$

$$g(x,y) = g(x-1,y) + s(x,y),$$

где s(x,y) — совокупное значение для каждой строки в прямоугольнике, начальное значение s(x, -1) = 0, а g(x, y) — начальное значение g(-1, y) = 0.

Вывод: Мы показали вам только основу, математический фундамент того, как искусственный интеллект понимает наш мир, естественно даже при таком прогрессе есть куда стремиться, будут разрабатываться все новые и новые модели поведения и обнаружения, но наша цель была показать вам что прежде всего за всем этим стоит математика.

УДК 519.172.3

ИСПОЛЬЗОВАНИЕ АЛГОРИТМА ASTAR ДЛЯ ПОИСКА ОПТИМАЛЬНОГО МАРШРУТА СЛЕДОВАНИЯ РОБОТОТЕХНИЧЕСКИХ УСТРОЙСТВ

Руселевич Д.Д., Трушко Я. Г.
Научный руководитель – Лебедева Г.И., к.т.н, доцент кафедры «Высшая математика»

В современном мире всё чаще и чаще используются различные, выполняющие широкий спектр задач робототехнические устройства. Для

ориентации в пространстве используются системы датчиков и сенсоров. Однако для ориентации на местности и для перемещения по ней простых данных недостаточно. Для этого используются различные алгоритмы. К примеру алгоритм A*(англ. A star) — алгоритм поиска, который находит во взвешенном графе маршрут наименьшей стоимости от начальной вершины до выбранной конечной.

Для работы алгоритма используется карта местности, составленная при помощи базы данных, хранящей в себе координаты объектов на плоскости.Зная координаты начальной и конечной точки можно найти путь следования (маршрут) устройства.

Принцип работы алгоритма. Имеются точки в декартовой системе координат: начальная точка А(0.0) и конечная точка Б(4.0). Для построения маршрута берутся точки с наименьшим весом (F).

В процессе работы алгоритма для точек рассчитывается функция F(v)=g(v)+h(v), где

g(v) —стоимость пути к текущей точке из начала пути, где v цена пути вдоль координат x,y.

h(v) — теоретическая стоимости пути из данной точки до конечной цели.

Фактически, функция F(v) — длина маршрута до цели, которая складывается из пройденного расстояния g(v)и теоретическиоставшегося расстояния h(v). Исходя из этого, чем меньше значение f(v), тем раньше мы откроем вершину v, так как через неё мы предположительно достигнем расстояние до цели быстрее всего. Открытые алгоритмом вершины можно хранить в очереди с приоритетом по значению f(v). A* действует подобно алгоритму Дейкстры и просматривает среди всех маршрутов ведущих к цели сначала те, которые благодаря имеющейся информации в данный момент являются наилучшими. Если же полученнаязначение функции F(v) в двух точках совпадает, тогда алгоритм далее выбирает произвольную точку и продолжает исследовать путь.

Использование данного алгоритма не требует большого количества производительных мощностей микроконтроллера устройств. Так же благодаря хранению точек в очереди возможно вычисление предположительной скорости, время затраченного на перемещение и текущие координаты устройства непосредственно при перемещении по маршруту, а так же изменение маршрута в режиме реального времени.

Так же используя данный алгоритм становится возможным совместная работа нескольких устройств. Зная текущие координаты устройств, можно обозначить их на карте как объект-препятствие и произвести перерасчёт маршрута следования каждого устройства в группе систем.

Литература

1. Yumeng YanResearch on the A Star Algorithm for Finding Shortest PathURL:https://www.researchgate.net/publication/370573811_Research_on_the_A_Star_Algorithm_for_Finding_Shortest_Path

2. Шагабазян. Д.В. Алгоритмы сортировки. Анализ, реализация, применение / Шагабазян. Д.В. , Штанюк А.А., Малкина Е.В. – Нижний Новгород: Нижегородский госуниверситет, 2019. – 42с.

УДК 681.3.06:519.248.681

ECDSA- И MQV-АЛГОРИТМЫ: ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

Кондратьев Д.П.
Научный руководитель – Бадак Б.А., старший преподаватель кафедры «Высшая математика»

Теория эллиптических кривых является неотъемлемым разделом алгебраической геометрии. Более того, она неразрывно связана с теорией чисел и комплексным анализом. Первооткрывателем свойств таких кривых считается древнегреческий ученый Диофант. Структуру группы на эллиптических кривых впервые ввёл французский математик Анри Пуанкаре. На протяжении долгого времени теория эллиптических кривых не имела применения, но в конце прошлого века она получила приложения в области построения алгоритмов факторизации больших чисел, а позднее и в криптографии. В 1985 году независимо друг от друга Нил Коблиц и Виктор Миллерпредложили использовать в криптографии алгебраические свойства эллиптических кривых. Это направление получило название **криптография на эллиптических кривых**(англ. EllipticCurveCryptography - ECC), или же эллиптическая криптография[1]. На сегодняшний день эллиптические кривые используются для нахождения факториалов чисел, для поиска и проверки простых чисел, в криптосистемах, в протоколах распределения ключей, в протоколах цифровой подписи и т.д.

Главное преимущество криптосистем, основанных на эллиптических кривых в сравнении с другими заключается в том, что сохраняется аналогичный уровень безопасности при более коротких ключах, однако существенным недостатком является высокая сложность вычислений, именно поэтомуисследования в этой сфере не прекращаются и довольно часто появляются новые алгоритмы.

Криптография существует уже более двух тысяч лет, однако свою популярность эта наука получила только в середине семидесятых годов