ЛИТЕРАТУРА

1. Гашков, С.Б. Задача об аддитивных цепочках и ее обобщения / С.Б. Гашков // Математическое просвещение, 2011, выпуск 15. С. 138-153.

2. Кнут, Д.Э. Искусство программирования / Д.Э. Кнут – 3-е изд. – М.: Вильямс, 2012. – 788 с.

УДК 519.171

Студ. М. Ю. Радченко, А. М. Карпач
Науч. рук. Е. В. Терешко
(кафедра высшей математики, БГТУ)

ЧТО ТАКОЕ ГРАФ? ПРИМЕНЕНИЕ ГРАФОВ В ПРОГРАММИРОВАНИИ

Если студент имеет цель стать хорошим специалистом в сфере своей специализации, ему необходимо разбираться во всех дисциплинах, преподаваемых в университете, в не зависимости, являются они предметами по специальности или нет. Именно поэтому проводить параллели и находить нечто общее между, на первый взгляд, ничем не схожими дисциплинами — одна из важнейших задач обучения. Тема «Графов» широко представлена в программировании и большинство программ, которые создаются студентами уже на 1 курсе, основаны, в том числе, и на математических графах.

Граф G — это упорядоченная пара G:=(V,E) , где V — это непустое множество вершин или узлов, а E — множество вершин, называемых рёбрами.

Вершины и рёбра графа называются также элементами графа, число вершин в графе — порядком, число рёбер — размером графа.

Граф может быть ориентированным или неориентированным. В ориентированном графе, связи являются направленными (то есть пары в E являются упорядоченными, например пары (1, 3) и (3, 1) это две разные связи). В свою очередь в неориентированном графе, связи ненаправленные, и поэтому если существует связь (1, 3) то значит что существует связь (3, 1).

Перед нами были поставлены вопросы: для чего нужны графы и что нужно знать, чтобы воспользоваться ими на практике при создании компьютерных программ?

Существует два способа представления графа: в виде списков смежности и в виде матрицы смежности. Оба способа подходят для представления ориентированных и неориентированных графов. И без труда представляются при помощи таких популярных языков программирования, как C++ или же JS.

При матрице смежности происходит заполнение квадратной матрицы A размером |V| x |V| (где V — количество вершин графа) следующим образом: A[i][j] = 1 (Если существует ребро из i в j) и A[i][j] = 0 (в обратном случае).

Вторым способом является список смежности. В данном представлении используется массив A, содержащий |V| списков. В каждом списке A[V] содержатся все вершины u, так что между V и u есть ребро.

В интернете, а также в специализированной литературе существует большое количество различных задач, решение которых представляется в виде графов. Часть из них основана на Гамильтоновом графе. Само название «гамильтонов цикл (граф)» произошло от задачи «Кругосветное путешествие», предложенной ирландским математиком Вильямом Гамильтоном в 1859 году. Нужно было, выйдя из исходной вершины графа, обойти все его вершины и вернуться в исходную точку.

В нашей работе была рассмотрена подобная задача и реализовано ее решение с использованием языка программирования C++.

В задаче имелось пять точек, соединенных определенных образом. Цель — посетить каждую только один раз.

Для написания кода была использована программа Visual Studio. После стандартного объявления используемых библиотек и основных переменных, в коде расположена первая основная часть программы — матрица смежности. Она составляется в виде двумерного массива A, в который входят целочисленные значения типа int — 1 или 0.

Основная функция кода main содержит небольшое меню приветствия. Здесь пользователю предоставляется возможность выбрать вершину, с которой будет начат путь. Далее на экран выводится матрица смежности для лучшего понимания задачи и выполняется переход на поиск решения. Этот переход обусловлен рекурсивной функцией gamilton(). Именно благодаря данному типу функции возможен поиск необходимого «пути движения» для решения поставленной задачи. Рекурсивная функция — это функция с такой организацией работы, при которой она вызывает сама себя.

Вся программа основана на условиях проверки и различных циклах, которые в конечном итоге выводят на экран оптимальное решение задачи, т.е. ряд чисел, каждое из которых значит определенную вершину гамильтонового графа.

Созданный код является универсальным, и, имея на руках любую задачу подобного типа, необходимо лишь изменить матрицу

смежности в самом начале программы. Дальнейшая работа уже не зависит от количества вершин и связей (ребер) между ними.

Из всего следует, что графы являются очень универсальным средством, которое помогает нам как в решении задач при изучении высшей математики, так и в программировании для написания наиболее оптимального кода. И умение сочетать различные дисциплины и изучать практические стороны различных тем — отличный способ совершенствоваться и достигать наилучшего результата.

ЛИТЕРАТУРА

1. Пацей, Н.В. Основы алгоритмизации и программирования: учеб.-метод. пособие для студентов специальности «Информационные системы и технологии (издательско-полиграфический комплекс)» / Н.В. Пацей. — Минск: БГТУ, 2010. — 289 с.

2. Новиков, Ф. А. Дискретная математика: Учебник для вузов. 3-е изд. Стандарт третьего поколения. — СПб.: Питер, 2017. — 334 с.

УДК 519.171

Студ. В. В. Хорхалёв
Науч. рук. И. К. Асмыкович
(кафедра высшей математики, БГТУ)

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ ПРИЛОЖЕНИЯ В КРИПТОГРАФИИ

На протяжении более сотни лет эллиптические кривые исследовались лишь узкими специалистами в области теории чисел. Но в 1985 г. одновременно и независимо Н. Коблиц и В. Миллер предложили использовать эллиптические кривые для построения криптосистем с открытым ключом. После этого интерес к эллиптическим кривым стремительно возрос. Эллиптические кривые применяются в разных областях криптографии таких, как теория кодирования, генерация псевдослучайных последовательностей, алгоритмическая теория чисел для построения тестов на простоту и, для создания метода факторизации целых чисел Ленстры.

Пусть F_q, $q = p^k$, конечное поле характеристики $p \geq 2$. Эллиптической кривой над полем F_q называется множество точек $(x, y) \in F_q \ RF_q$, удовлетворяющих уравнению Вейерштрассе [1]:

$$y^2 + ay + b = x^3 + cx^2 + dx + e.$$

К множеству точек эллиптической кривой также добавляется точка, называемая точкой в бесконечности и обозначаемая символом ∞. Если характеристика поля $p \geq 3$ (а мы будем рассматривать именно этот случай), уравнение, путем замены переменных, может быть