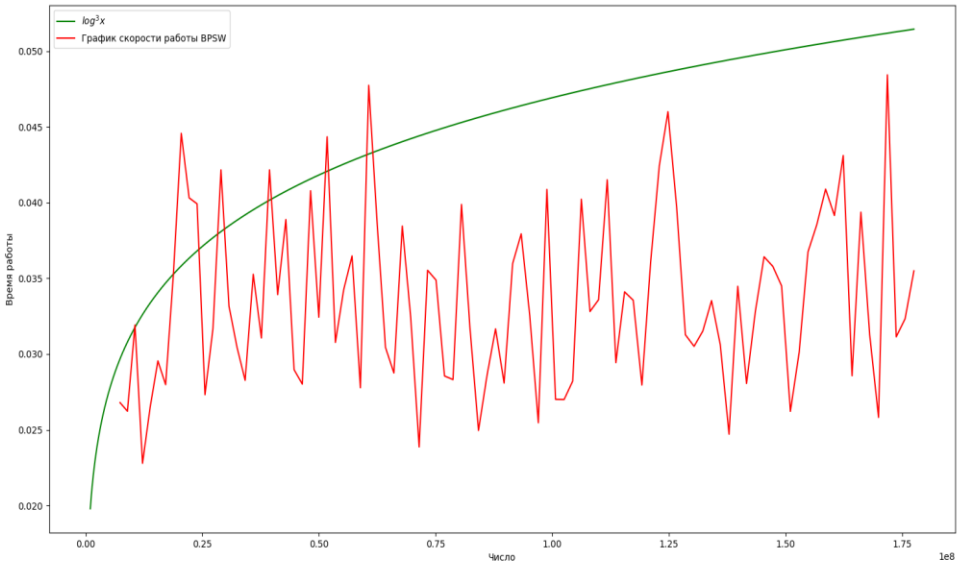


Рисунок 1 — График зависимости скорости работы алгоритма BPSW от размера простого числа

Список использованных источников:

1. Factorization of a 768-bit RSA Modulus / Th. Kleinjung [et al.] // Advances in Cryptology — CRYPTO 2010 : 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15—19, 2010. — Santa Barbara, 2010. — P. 333—350.
2. Бараш, *Л. Ю.* Алгоритм AKS проверки чисел на простоту и поиск констант генераторов псевдослучайных чисел / Л. Ю. Бараш // Безопасность информационных технологий. — 2005. — №2. — С. 27—38.
3. Шнайер, Б. Прикладная криптография / Б. Шнайер ; пер. с англ. — М. : Триумф, 2013. — 816 с.

ВИЗУАЛИЗАЦИЯ РЕШЕНИЙ НЕКОТОРЫХ МАТЕМАТИЧЕСКИХ ЗАДАЧ В MAPLE

Кузнечик В. А., Милинкевич М. И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

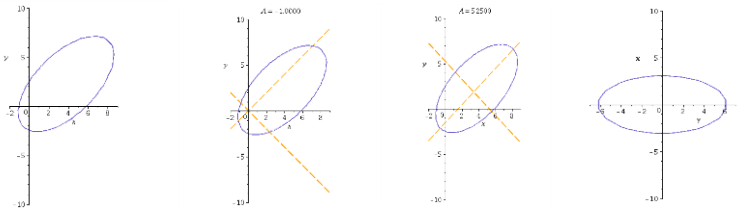
Калугина М. А. - к. ф.-м. н., доцент

В работе представлены результаты изучения средств и технологий системы компьютерной алгебры Maple и их применения для визуализации решений некоторых математических проблем. Перечислены примеры задач, для которых созданы процедуры поэтапного решения с элементами анимации: приведение уравнений кривых и поверхностей второго порядка к каноническому виду, разложение функции в ряд, решения систем дифференциальных уравнений, решение краевой задачи на колебания поверхности барабана и построение векторного поля.

Наглядность поставленной задачи является важной частью не только для понимания процесса решения, но и для исследования его в динамике, которая легче воспринимается зрительно. Анимация этапов решения, кроме этого, даёт выразительное представление о скорости явления. Студентам визуализация позволяет находить закономерности, систематизировать найденные решения и моделировать определённую ситуацию при исследовательской работе.

Одной из задач, геометрический смысл которой полезен при обучении и на практике, является задача приведения кривых и поверхностей второго порядка к каноническому виду. Ниже приведено ее решение на примере эллипса, заданного уравнением $5x^2 - 6xy + 5y^2 - 24x - 32 = 0$ (рис. 1 а), реализованное с помощью созданной процедуры. Для решения этой задачи в Maple можно построить матрицу квадратичной формы левой части уравнения, затем с помощью команд *EigenVectors* и *GramSchmidt* из пакета *LinearAlgebra* найти ее собственные векторы, из которых построить ортонормированный базис. Таким образом, получается базис, образованный поворотом исходного на некоторый угол (рис. 1 б). Ещё одним действием можно продемонстрировать параллельный перенос

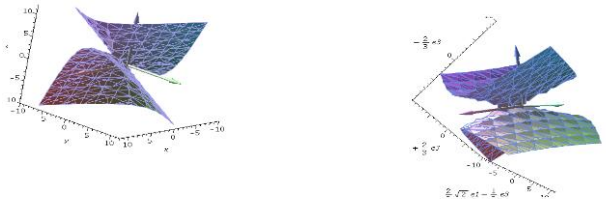
центра построенного базиса в точку канонической системы эллипса (рис. 1 в). При выбранном порядке базисных векторов получен эллипс, у которого параметры связаны отношением $b > a$, поэтому, изменив его, можно получить классический вид эллипса (рис. 1 г) с уравнением $\frac{8}{77}Y^2 + \frac{2}{77}X^2 = 1$.



а) б) в) г)

Рисунок 1 — Изображение эллипса в разных базисах

Аналогично можно визуализировать переход к базису из собственных векторов для поверхности второго порядка (рис. 2). На примере уравнения $3x^2 - 7y^2 + 3z^2 + 8xy - 8xz - 8yz + 10x - 14y - 6z - 8 = 0$ получено каноническое уравнение $9X^2 + Y^2 - 9Z^2 = 1$. Это уравнение однополостного гиперболоида. В Maple сразу показаны преобразования по осям.



а) б)

Рисунок 2 – Однополостный гиперболоид в «старом» и «новом» базисах

На рисунке 3 а) в одной системе координат изображены графики частичных сумм разложений заданной функции в ряды Тейлора и Фурье (по тригонометрической системе функций и по многочленам Чебышёва и Лежандра). Кроме этого, Maple предоставляет возможности 3D-анимации разложения функции двух аргументов в ряд Тейлора (рис. 3 б).

а) б)

Рисунок 3 — Графики аппроксимирующих функций

С помощью Maple удобно визуализировать решение задачи Коши для систем дифференциальных уравнений первого порядка. Важным для понимания является геометрический смысл дифференциального уравнения. Пакет DEtools предоставляет функционал для построения поля направлений дифференциального уравнения с возможностью анимации данного процесса (рис. 4).

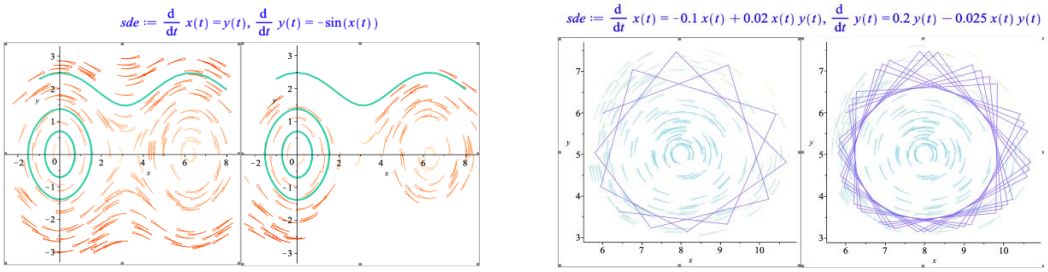
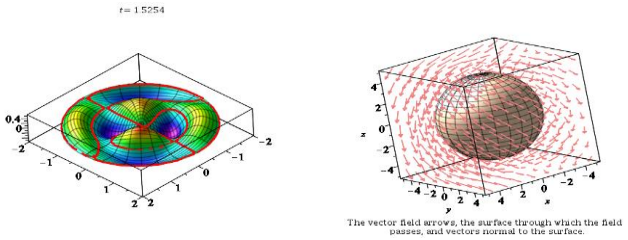


Рисунок 4 — Решения систем дифференциальных уравнений в поле направлений



а) б)

Рисунок 5 — Демонстрация решения других задач в Maple

В завершение приведён ряд других задач, визуализация решения которых возможна в Maple. Например, удалось построить процедуру для анимации колебаний поверхности барабана, которые описываются с помощью функций Бесселя (рис. 5 а). С помощью функций, расположенных в пакете Student[VectorCalculus], удалось построить векторное поле, проходящее через поверхность сферы (рис. 5 б).

Приведённые выше примеры затрагивают темы, которые часто встречаются студентам на практике, и это лишь малая часть задач, решение которых можно визуализировать с помощью Maple.

Список использованных источников:

1. Garvan, Frank (Frank G.), 1955-The Maple book / by Frank Garvan. p. cm.Rev. ed. of: Maple V primer. C1997. Includes bibliographical references and index. ISBN 1-58488-232-8 (alk. paper) 1. Maple (Computer file) 2. Algebra—Data processing. I. Garvan, Frank (Frank G.), 1955- Maple V primer. II. Title.

2. Maplesoft [Электронный ресурс]. – Режим доступа : https://www.maplesoft.com/support/help/Maple/view.aspx?path=worksheet%2freference%2fPlottingGuide

НЕЙРОННЫЕ СЕТИ ДЛЯ ПРОГНОЗИРОВАНИЯ РЕЗУЛЬТАТОВ СОРЕВНОВАНИЙ ПО КИБЕРСПОРТИВНЫМ ДИСЦИПЛИНАМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Минчук С. Г.

Жвакина А. В. – канд. техн. наук, доцент

Последнее время все больше растет популярность киберспортивных дисциплин. С каждым годом проводится огромное количество соревнований по всему миру. В некоторых дисциплинах основными навыками, которыми должны обладать игроки, являются скорость, реакция и внимание игроков, в других же, важна именно стратегия. Из-за того, что в этих играх есть большое количество комбинаций, которые можно использовать, мы можем рассматривать их в качестве модели для прогнозирования результатов по ним. Исходя из того, что некоторые киберспортивные дисциплины включены в список настоящих видов спорта, это дает возможность рассматривать их не просто как развлечение, а как серьезное мероприятие.

Прогнозирование результатов игры основывается на определении степени развития конкретного объекта или команды в целом, а также количество ранее произошедших событий. Таким образом мы анализируем состояние объекта, базируясь на его текущих характеристиках или их совокупности, которые произошли ранее и которые происходят в данный момент. Для прогнозирования исхода выбран многослойный перцептрон. Многослойный перцептрон или сети прямого распространения как правило имеют три отличительных признака: - каждый нейрон имеет гладкую (всюду дифференцируемую) нелинейную функцию активации; - сеть содержит один или несколько слоев скрытых нейронов; - сеть имеет высокую степень связности, которая реализуется посредством синаптических соединений. Установлено, что многослойный персептрон имеет достаточную точность и скорость для прогнозирования временных рядов [2].

Многослойный перцептрон состоит из следующих частей (рис.1):

- вход (*input*) нейронной сети;
- выход (*output*) нейронной сети;
- скрытые, слои с большим количеством синаптических соединений.