****

**APPLICATIONS OF POLYNOMIAL INTERPOLATION**

REPORT BY – KRISHNAPRIYA PANICKER

COURSE TITLE - LINEAR ALGEBRA

PROJECT GROUP – 8

INSTITUTE - INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY, HYDERABAD

DATE – 21st November 2020

ABSTRACT

In this work, starting from understanding the basics of polynomial interpolation we move onto the areas where the polynomial interpolations are applied. Here we have explored some of the applications of polynomial interpolations such as Karatsuba algorithm, Tom-cook multiplication, Secret Sharing schemes, and Secret multi party computations. We have focused upon the usage of linear algebra in these areas.

# **Introduction**

Polynomial Interpolation is a method of estimating values between the known data points. When graphical data contains a gap, but data is available on either side of the gap or at a few specific points within the gap, an estimate of values within the gap can be made by the interpolation. The simplest method of interpolation is to draw straight lines between the known data points as the combination of those straight lines. This method is also called as the linear interpolation. A more precise approach uses a polynomial function to connect the points. A polynomial is a mathematical expression comprising a sum of terms, each term including a power and multiplied by a coefficient.

**1.1 DEFINITION**

Given a set of n+1 data points (xi, yi) where no two xi are the same, a polynomial is said to interpolate the data if for each .

**Polynomial Interpolation Theorem:**

Suppose that we have points:

Where are distinct numbers (no such condition on the ’s). Then there is exactly one polynomial of degree that interpolates these points i.e.

for

**Proof 1:** The conditions for can be written as a linear system in terms of the coefficients of the polynomial:

**V b = y**

Where b=T is the vector of coefficients to be determined, y= and

V=

One may also check by induction that V has determinant

|V|= --- (1)

V is an important matrix that is useful elsewhere also. This matrix is known as **Vandermonde matrix.**  Vandermondematrixisa matrix with the terms of a geometric progression in each row, i.e an m n matrix. The above given equation (1) is called the Vandermonde determinant or Vandermonde polynomial. This matrix is non-zero if and only if all are distinct. Since all the xi ‘s are all distinct (as per theorem), this implies that V is nonsingular, completing the proof. Thus the polynomial interpolation is proved.

One more proof can be provided for the above theorem:

**Proof 2:** Suppose we interpolate through data points with an at-most degree polynomial (we need at least n+1 data points or else the polynomial cannot be fully solved for). Suppose also another polynomial exists also of degree at most that also interpolates the points, call it q(x).

Consider. We know,

1. Has degree at most, since and are no higher than this and we are just subtracting them.
2. At the

Therefore r(x) has n+1 roots.

But *r*(*x*) is a polynomial of degree ≤ *n*. It has one root too many. Formally, if *r*(*x*) is any non-zero polynomial, it must be writable as{\displaystyle r(x)=A(x-x\_{0})(x-x\_{1})\cdots (x-x\_{n})}, for some constant *A*. By distributivity, the *n* + 1 *x'*s multiply together to give leading term{\displaystyle Ax^{n+1}}, i.e. one degree higher than the maximum we set. So the only way *r*(*x*) can exist is if *A* = 0, or equivalently, *r*(*x*) = 0.

{\displaystyle r(x)=0=p(x)-q(x)\implies p(x)=q(x)}So *q*(*x*) (which could be any polynomial, so long as it interpolates the points) is identical with *p*(*x*), and *q*(*x*) is unique.

**Construction of interpolation polynomial**

From above two proofs, we have found that there exists unique polynomial of degree that interpolates points. So these polynomials can be found by different methods. Such methods are:

1. Using Vandermonde matrix:

* Suppose that the interpolation polynomial is in the form:

The statement that p interpolates the data points means that for each . If we substitute equation (1) in here, we get a [system of linear equations](https://en.wikipedia.org/wiki/System_of_linear_equations) in the coefficients *ak*. The system in matrix-vector form reads the following [multiplication](https://en.wikipedia.org/wiki/Matrix_multiplication):

=

We have to solve this system for *ak.* to construct the interpolant p(x). After solving the above matrix we would get the unique polynomial.

1. Lagrange’s formula

* Lagrange devised a technique by which one may immediately construct a interpolating polynomial. The formula goes as such :

Li (x) =

Here the numerator is the product of all the terms of the form (x-xj) for ji. The denominator is the same as the numerator, except that the x is replaces by xi.

1. Newton’s divided difference

* This method is another way by which interpolating polynomial for a given set of points can be found. Whether we use newton’s divided difference or Lagrange’s method the answer is always same. We define the divided differences of as follows:

1. 0-th order divided difference:
2. 1st order divided difference:
3. 2nd order divided difference:
4. Similarly kth order divided difference:

So one by one divided differences are found and then the interpolating polynomial is found. These were the three ways by which the interpolating polynomial would be found.

Now we would look upon some of the applications of polynomial interpolations.

Applications of Polynomial Interpolations:

There are few areas where the polynomial interpolation are widely used or form the basis for the different algorithms. Here I am going to explain about one such application of the polynomial interpolation in which it forms the basis for those algorithms.

**Numerical methods for solving linear differential equations**

Polynomial interpolation forms the basis for the algorithm of the numerical ordinary differential equations.

First of all let us understand what numerical methods for differential equations are. Numerical methods for ordinary differential equations are methods used to find the numerical approximations to the solutions of differential equations. A differential equation is an equation for a function that relates the values of the function to the values of its derivatives. An ordinary differential equation is a differential equation for a function of single variable. Every discretization method turns your differential equation into a finite set of equations (a problem in “algebra”). This is so for boundary value problems as well as initial value problems. The point of discretization is to construct an algebraic problem which can be solved in finite time. Of course, the algebraic solution will only be an approximation to the solution of the differential equation. If the original differential equation is linear, your discrete problem will also be linear, so you have a problem within linear algebra. If the problem is nonlinear, however, you will have to use some iterative technique (usually Newton's method) to find the approximate solution. But even Newton's method will only lead to a sequence of linear algebraic problems to be solved.

Limitations: Only the ordinary differential equations that are linear can be solved using linear algebra.

The different methods to solve a system of linear differential equations .Let the general system of homogeneous differential equation is given by:

Where the coefficients are arbitrary functions of t. The system is most often given in a shorthand format as a matrix-vector equation in the form:

=

Where the matrix of coefficients, A, is called the coefficient matrix of the system. The vectors are:

= and x=

Methods to solve this:

1. **Distinct real eigenvalues** **:**

* For solving the system of equations, let us assume x (t) =are independent of t. Upon substitution we obtain

**λA;**

and upon cancellation of the exponential, we obtain the eigenvalue problem

**Av=λv.**

Finding the characteristic equation of the matrix A by **det (A- λI) = 0.**From these we get the corresponding eigenvectors. To determine the corresponding eigenvectors, we substitute the eigenvalues successively into **(A- λI) v = 0.**We will write the corresponding eigenvectors v1 and v2 using the matrix notation if there are two equations only:

Using the principle of superposition, the general solution to the ode is therefore:

**x (t) = c1v1 + c2v2**

Or explicitly writing out the components,

**x1(t) = c1v11 + c2v21**

**x2(t) = c1v12 + c2v22**

We will see the above method using one example of two equations:

**Example: Find the general solution of x˙1 = x1 + x2, x˙2 = 4x1 + x2.**

The equation to be solved may be rewritten in matrix form as:

= ------ (1)

Eigen values of this matrix can be found as:

Det (A − λI) = 0

λ2 - 2λ -3=0

(λ - 3)(λ+1)=0

**λ**=3 or λ=-1

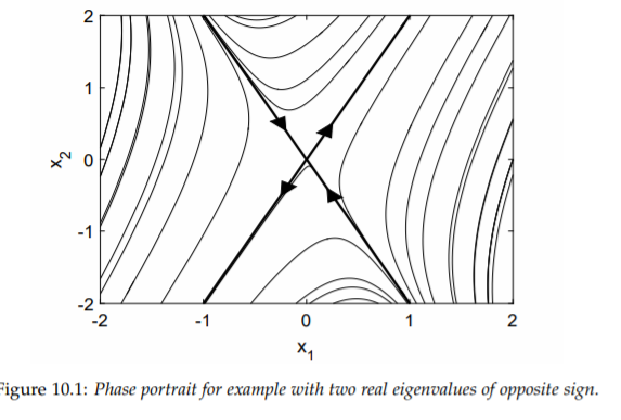
For eigenvalues their eigenvectors are as follows:

For **λ**1 = 3, v1=; **λ**2 = -1, v1= , so the general solution of the ode is: x (t) = c1v1 + c2v2

or explicitly writing out the components,

x1 (t) = c1 + c2

x2 (t) = 2c1 - 2c2

****

1. **Repeated eigenvalues with one eigenvector**

* We will see this using an example:

**Example: Find the general solution of x˙1 = x1 - x2, x˙2 = x1 + 3x2.**

The equation to be solved may be rewritten in matrix form as:

* = ------ (1)

Eigen values of this matrix can be found as:

Det (A − λI) = 0

λ2 - 4λ +4=0

(λ - 2)2=0

**λ**=2

Therefore here λ=2 is a repeated eigenvalue. The associated eigenvector is found as

**λ=2, v=;**

The general solution for the ode goes as x (t) = c1.But this is only the first solution we need to find the second solution to be able to satisfy the initial conditions. For that let us take

x = (w+tv) where λ and v is the eigenvalue and eigenvector of the first solution and w needs to be determined. For this we substitute into = Ax**,** assuming Av=λv and cancelling out the exponential, we get

**v + λ (w + tv) = Aw + λtv**.

v + λ w + λ tv = Aw + λtv

(A- λI) w=v.

If A has only a single linearly independent eigenvector v, then (10.13) can be solved for w (otherwise, it cannot). Using A, λ and v of our present example, (10.13) is the system of equations given by:

=

The first and second equation are the same, so that. Therefore,

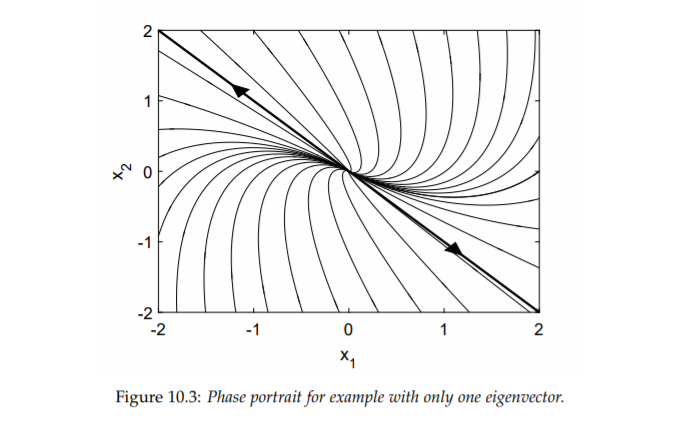
w=

=

Notice that the first term repeats the first found solution, i.e., a constant times the eigenvector, and the second term is new. We therefore take w1 = 0 and obtain

w=

Thus the solution obtained is as: x2 (t) = c2

****

1. **Solution by diagonalization:**

* The homogeneous equations can be solved by another method which is by using diagonalization. With = Ax, we suppose A can be diagonalized using

**S-1AS= Λ ------(1)**

Where Λ is the diagonal eigenvalue matrix, and S holds the eigenvectors. We can change the variables in = Ax using **x=Sy** and obtain **.**

Multiplication on the left by **S-1** and using (1) results in

**y= Λy**

This when solved gives the final solution.

This can be understood by an example:

**Example:**

= ----- (1)

Here **S=, so Λ=**

**=**

**=**

And the uncoupled y-equations are given by:

**=3, = -**

With solution y1 (t) = c1, y2 (t) = c2

Transforming back to the x-variables, we have,

=

Thus the solution obtained is as follows:

x1 (t) = c1 + c2

x2 (t) = 2c1 - 2c2