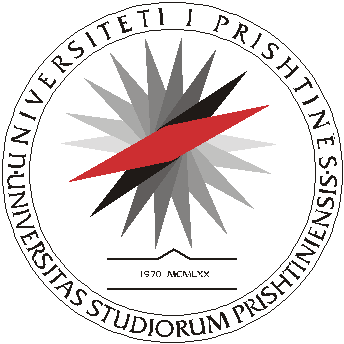
**UNIVERSITETI I PRISHTINËS**

**“Hasan Prishtina”**

**Fakulteti i Shkencave Matematike – Natyrore  
Shkencë Kompjuterike**



**INTERPOLIMI & POLINOMI I LAGRANZHIT**

**Studentet: Mentori:**

**Diellza Bytyçi Eliot Bytyçi  
Drita Shujaku**

**Interpolimi**

Interpolimi si term është përfitimi(llogaritja) e një vlere të panjohur në mes të vlerave që janë të njohura në një varg të vlerave, ose nxjerrja e të dhënave nga disa që dihen.

Shpesh në inxhinieri dhe në shkencë, përgjithësisht kemi një numër të pikave, që janë të fituara nga ndonjë eksperiment, që paraqet vlerat e një funksioni për një numër të limituar të vlerave dhe shpesh kërkohet të interpolohet(fitohet) vlera e këtij funksioni për një vlerë të ndërmjetme.

Polinomet mund të përdoren për të përafruar lakore të kompilkuara. Një aplikim është tek logaritmi natyral dhe funksionet trigonometrike(lakoret fitohen me anë të polinomit).

Një arsye e fortë që të përdoren përafrimet e funksioneve me anë të polinomeve është sepse llogaritja e derivateve dhe integralit të pacaktuar ëshët më lehtë te polinomet

Një problem i natyrës së njejtë që lidhet me interpolimin është përafrimi i një funksioni të komplikuar me një të thjeshtë. Disa pika që dihen prej funksionit fillestar(të ndërlikuarit) mund të përdoren për të krijuar një interpolim në një funksion më të thjeshtë. Sigurisht, kur një funksion i thjeshtë është përdorur për të përafruar këto pika, gabimet interpoluese janë zakonisht prezente.

Janë disa metoda të ndryshme të interpolimit. Ndër më të rëndësishmet janë: Interpolimi Linear dhe Interpolimi Polinomial.

Interpolimi linear është metoda më e thjeshtë e interpolimit. Vizaton disa drejteza mes pikave të dhëna dhe funksionin e merr si kombinim të këtyre drejtëzave.

Interpolimi linear është i shpejtë dhe i lehtë, por gabimi I llogaritjes është proporcional me katrorin e distancës mes pikave të dhëna.

Interpolimi polinomial përdoret në analize numerike për të gjetur një polinom që kalon në disa pika të dhëna.

Një polinom është një shprehje matematikore, si shumë e termave, secili term përmban një variabël në një fuqi dhe të shumëzuar me një koeficient.

Një ndër klasët më të njohura të funksioneve janë polinomet algjebrike, një bashkësi e funksioneve të trajtës:

Ku *n* është numër pozitiv dhe janë konstanta. Rëndësia e polinomeve është se përafrojnë funksionet e *vazhdueshme*.

Pra çdo funksion i cili është i vazhdueshëm në një interval të mbyllur dhe të kufizuar, ekziston një polinom që është i përafërt me funksionin.

Nëse një bashkësi e të dhënave përmban *n* pika(që i dihet vlera), atëherë ekziston saktësisht një polinom i shkallës *n-1* ose më të vogël që kalon në ato pika.

Në analize numerike, ndër metodat për interpolim polinomial është edhe metoda e Lagranzhit.

Interpolimi polinomial i Lagranzhit që kalon neper dy pika () dhe (), quhet interpolim polinomial linear dhe shënohet:

Kjo formulë përdoret në rastet e interpolimit linear, pra kur janë dy pika të dhëna, dhe polinomi i përafrohet ekuacionit të drejtezes që kalon nëper dy pika.

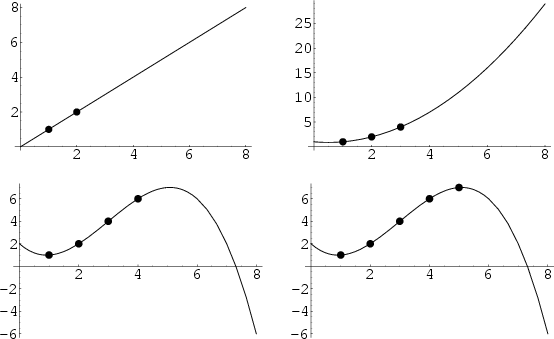


Fig. 1: Funksionet(polinomet e shkallës që kalojn nëpër pikat

Por meqë ky interpolim kishte gabime më të mëdha gjatë përafrimit, merret zakonisht një numër më i madh i pikave, ku mundësia për gabim është më e vogël.

Për përgjithësim të interpolimit, marrim parasysh polinomin e shkallës, më së shumti *n*, që kalon neper pika

Në këtë rast së pari ndërtojmë një funksion , për , ashtu që kur dhe .

Që të plotësohet kushti që për cfardo , kërkohet që numëruesi i të përmbaj termin

Që të plotësohet , emeruesi i duhet të jetë :

=

Interpolimi polinomial gjendet lehte nëse dihet . Ky polinom, i quajtur interpolimi polinomial i -të I Lagranzhit, është përcaktuar me anë të teoremës në vijim:

Nëse janë numra të ndryshëm dhe është një funksion, ku vlerat e funksionit janë dhënë në pikat e dhëna, atëherë ekziston një polinom i vetëm , i shkallës jo më të madhe se , ashtu që

, për cdo .

Ky polinom është dhënë me

,   
  
ku për çfarëdo

Problemi kryesor që paraqitet me interpolimin polinomial është kur, edhe pse ekziston një funksion polinomial i cili kalon nëpër të gjitha pikat që janë dhënë, grafi(lakorja) mund të mos jetë ajo që kërkohet. Është e mundshme që një funksion polinomial, edhe pse në ato pika përputhet, mund të ndryshoj në disa vlera mes këtyre pikave, në rast se ka maksimume ose minimume të theksuara.

**Aplikimi i Polinomeve të Lagranzhit**

Polinomet e Lagranzhit përdoren në integrimin numerik për të ndërtuar formulat e Neëton–Cotes. Këto polinome mund të llogariten edhe në fusha të fundme duke i bërë të aplikueshme në kriptografi. Një shembull i tillë paraqet Skemen e Shamirit për Ndarjen e Sekretit(Shamir's Secret Sharing scheme):

Njëmbëdhjetë shkencëtarë punojnë në një projekt sekret. Ata duan që t’i kyçin dokumentet në një kabinet ashtu që kabineti të mund të hapet vetëm nëse gjashtë ose më shumë shkencëtar janë të pranishëm. Për raste të tilla, Adi Shamir propozoi një skemë për menaxhimin e çelësave kriptografik. Në mënyrë që t’i mbrojmë të dhënat, mund t’i enkriptojmë ato, por për mbrojtjen e çelësit enkriptues nevojitet metodë tjeter. Mënyra më e besueshme do të ishte përdorimi i skemës , për , me ç’rast do të mund të gjejmë çelësin origjinal edhe nëse e pjesëve shkatërrohen, por armiqtë tanë nuk do arrinin të ndërtojnë çelësin edhe nëse do t’i gjenin nga pjesët e mbetura.

Qëllimi është që sekreti S të ndahet në pjesë , ashtu që:

1. Njohja e çfarëdo ose më shumë pjesëve mundëson llogaritjen e lehtë të .
2. Njohja e ose më pak pjesëve nuk zbulon vlerën e .

Kjo skemë quhet skema threshold . Nëse atëherë të gjithë pjesëmarrësit duhet të rindërtojnë sekretin.

**Skema e Shamirit për shpërndarjen e sekretit**

Kjo skemë bazohet në idenë që 2 pika janë të mjaftueshme për të definuar në vijë, 3 pika mjaftojnë për të konstruktuar një parabollë, 4 pika për lakoren kubike, e kështu me radhë. Pra, nevojiten pikë për të definuar një polinom të shkallës .

Supozojmë që dëshirojmë të përdorim një skemë për të shpërndarë sekretin , element i fushës së fundme të madhësisë , ku ; dhe është një numër i thjeshtë.

Zgjedhim numra natyral të rastësishëm , ku dhe . Ndërtojmë polinomin dhe pikat, për shembull caktojmë , që të gjejmë . Çdo pjesëmarrësi i jepet një pikë (pika hyrëse në polinom dhe rezultati dalës). Nga cilado nënbashkësi e çifteve , mund të gjejmë koeficientët e polinomit duke përdorur interpolimin. Sekreti është termi konstant . Kjo zbatohet duke shfrytëzuar vetinë e interpolimit, ku për çifte , për të ndryshme, ekziston një polinom unik i shkallës , që kalon nëpër të gjitha pikët.

**Perdorimi**

Shembulli i mëposhtëm paraqet idenë e kësaj skeme, duke përdorur aritmetiken e numrave të plotë dhe jo atë të fushës së fundme.

Supozojmë që sekreti ynë është 1234, pra .

Dëshirojmë të ndajmë sekretin në 6 pjesë , ku cilado nënbashkësi e 3 pjesëve është e mjaftueshme për të fituar sekretin. Marrim 2 numra të rastësishëm: 166 dhe 94.

(; ; )

Kështu polinomi jonë për të krijuar pikët do të jetë:

Ndërtojmë 6 pikët nga polinomi:  
; ; ;; ;  
. Secilit nga pjesëmarrësi i japim njërën nga pikët.

Për t’a rindërtuar sekretin na mjaftojnë 3 pika të çfarëdoshme. Kështu marrim:  
; ;

Llogarisim polinomet e Lagranzhit:

Prandaj

Sekreti është koeficienti i lirë, që do të thotë se .  
Edhepse kjo metodë funksionon, në këtë detyrë ka një mangësi sigurie për shkak të mos përdorimit të aritmetikes së fushës së fundme. Megjithatë ne nuk do të përfshijmë zgjidhjen e këtij problemi në këtë seminar.

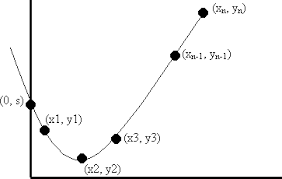
****

Fig. 2: Skema e ndarjes së sekretit - Polinom i shkallës ()

# Referencat

Optimal systems of nodes for Lagrange interpolation on bounded intervals. (2001). *Journal of Computational and Applied Mathematics*, 325–341.

*Polynomial interpolation*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Polynomial\_interpolation

Shamir, A. (1979). How to Share a Secret.

*Shamir's Secret Sharing*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Shamir%27s\_Secret\_Sharing

Thévenaz, P., Blu, T., & Unser, M. (n.d.). Interpolation Revisited. 2000.

# Tabelae figurave

[Fig. 1: Funksionet(polinomet e shkallës që kalojn nëpër pikat 3](#_Toc451700470)

[Fig. 2: Skema e ndarjes së sekretit - Polinom i shkallës () 7](#_Toc451700471)