Bevezetés az algebrába 1

Polinominterpoláció

Wettl Ferenc diáinak felhasználásával

Lagrange tétele

Feladat: Adva van $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in K$, ahol K test, és $x_1, \ldots, x_n$ különbözők. Keressünk olyan $f \in K[x]$ polinomot, melyre $f(x_i) = y_i$ $(i = 1, 2, \ldots, n)$.

Geometriailag $K = \mathbb{R}$-re: Adva van a koordinátarendszerben n pont, amelyeknek a vízszintes koordinátájuk különböző. Olyan polinomot keresünk, amelynek a grafikonja keresztülmegy az előírt pontokon.

P (x_1, y_1)-hez jó az y_1 konstans polinom (grafikonja egy vízszintes egyenes).

Két ponthoz találunk egy (legföljebb) elsőfokú polinomot (grafikonja egy nem feltétlenül vízsszintes egyenes)

Három ponton, ha nincsenek egy egyenesen, keresztülvezethető egy parabola.

Mj Ha van ilyen f polinom, akkor ∞ sok van, mert $f(x) + g(x)\prod_{i=1}^{n}(x - x_i)$ is jó tetszőleges $g(x) \in K[x]$ polinomra.

Lagrange-interpoláció

T **Lagrange-interpoláció**

K test, $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in K$, $\quad x_1, \ldots, x_n$ különbözők.
Ekkor pontosan egy olyan legfeljebb $n-1$-edfokú $f \in K[x]$ polinom létezik, melyre $f(x_i) = y_i$ $(i = 1, 2, \ldots, n)$.

B (Létezés) Először elkészítjük a Lagrange-alappolinomokat az adott $x_1, \ldots, x_n$ helyekhez.

$$L_i(x) = \frac{(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_n)}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)}$$

$$L_i(x_j) = \begin{cases} 1, & \text{ha } i = j, \\ 0, & \text{ha } i \neq j. \end{cases} \qquad \rightsquigarrow \qquad f(x) = \sum_{i=1}^{n} y_i L_i(x) \text{ megfelel.}$$

(A tétel szerinti f a Lagrange-féle interpolációs polinom)

(Egyértelműség) Ha f és g is ilyen, akkor a $h(x) = f(x) - g(x)$ polinomnak gyöke $x_1, \ldots, x_n \Rightarrow$
$(x-x_1)\cdots(x-x_n) \mid h(x)$, de $\deg h \leqslant n-1 \Rightarrow h = 0$, azaz $f = g$.

P

x_k	-1	0	1	2
y_k	-5	5	5	7

M

$$L_1(x) = \frac{(x)(x-1)(x-2)}{(-1)(-1-1)(-1-2)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 - \frac{1}{3}x$$

$$L_2(x) = \frac{(x+1)(x-1)(x-2)}{(0+1)(0-1)(0-2)} = \frac{1}{2}x^3 - x^2 - \frac{1}{2}x + 1$$

$$L_3(x) = \frac{(x+1)(x)(x-2)}{(1+1)(1)(1-2)} = -\frac{1}{2}x^3 + \frac{1}{2}x^2 + x$$

$$L_4(x) = \frac{(x+1)(x)(x-1)}{(2+1)(2)(2-1)} = \frac{1}{6}x^3 - \frac{1}{6}x$$

$$-5L_1 + 5L_2 + 5L_3 + 7L_4 = 2x^3 - 5x^2 + 3x + 5$$

Newton-interpoláció

Az interpoláció feladatát megoldhatjuk úgy is, hogy először az első számpárhoz adunk interpoláló (konstans) polinomot, ezt módosítjuk, hogy a második számpárhoz is jó legyen, stb.

Ha $f_k(x)$ jó az első k számpárhoz (és $\deg f_k < k$), akkor

$$f_{k+1}(x) = f_k(x) + c_k(x - x_1)(x - x_2)\cdots(x - x_k) \qquad (c_k \in K)$$

is kielégíti az első k feltételt, és c_k választható úgy, hogy a $(k+1)$-ediket is kielégítse:

megoldjuk az $y_{k+1} = f_k(x_{k+1}) + (x_{k+1} - x_1)\cdots(x_{k+1} - x_k)c_k$ egyenletet az ismeretlen c_k paraméterre (az együtthatója nem nulla).

Továbbá $\deg f_{k+1} \leqslant k$ is teljesül.

Mj A Newton-interpoláció előnye:

- Kisebb fokú polinomokkal kell dolgoznunk, mintha rögtön n alappolinomot gyártunk.
- Ha egy függvényt interpolálunk mérési eredmények alapján, finomíthatjuk az interpolációt új helyek hozzáadásával.

P Oldjuk meg ismét az előző feladatot:

x_k	-1	0	1	2
y_k	-5	5	5	7

m $f_1(x) = -5$

$$f_2(x) = -5 + c_1(x+1)$$
$$5 = -5 + c_1(0+1)$$
$$c_1 = 10$$
$$f_2(x) = 10x + 5$$

$$f_3(x) = 10x + 5 + c_2(x+1)x$$
$$5 = 15 + c_2 \cdot 2 \cdot 1$$
$$c_2 = -5$$
$$f_3(x) = -5x^2 + 5x + 5$$

$$f_4(x) = -5x^2 + 5x + 5 + c_3(x+1)x(x-1)$$
$$7 = -5 + c_3 \cdot 3 \cdot 2 \cdot 1 \Rightarrow c_3 = 2$$
$$f(x) = f_4(x) = 2x^3 - 5x^2 + 3x + 5$$

Lagrange tétele

Polinominterpoláció véges testek fölött

T Minden $f : \mathbb{Z}_p \to \mathbb{Z}_p$ függvény polinomfüggvény, és ∞ sok különböző polinommal megadható.

B Az $(i, f(i))$ $(i = 0, 1, \ldots, p-1)$ értékekhez van interpoláló polinom, és ehhez $x(x-1)(x-2)\cdots(x-(p-1))$ tetszőleges polinomszorosát hozzáadhatjuk.

Mj $x(x-1)\cdots(x-(p-1)) = x^p - x$, ugyanis a kis Fermat-tétel szerint $\mathbb{Z}_p$ minden eleme gyöke $(x^p - x)$-nek, s mivel ez már p darab különböző gyök, más gyöke nem is lehet az $x^p - x$ polinomnak.

F Egy széf kódja egy $[0, p-1]$-be eső egész, ahol p prím. Osszuk meg ezt $n < p$ ember közt úgy, hogy közülük bármelyik 3 ki tudja nyitni a széfet, de semelyik 2 ne tudjon meg a kódról semmit.

M Legyen $f \in \mathbb{Z}_p[x]$ egy másodfokú polinom, a széf kódja legyen $f(0)$. A k-adik embernek adjuk oda $f(k)$ értékét ($k = 1, 2, \ldots, n$). Bármely 3 ember a három (i, y_i), (j, y_j), (k, y_k) párból egyértelműen fel tudja írni f-et, amiből megkapja $f(0)$-t, de 2 ember nem tud meg a kódról semmit, mert minden $t \in \mathbb{Z}_p$ értékre pontosan egy legföljebb másodfokú polinom van, melynek grafikonja átmegy az (i, y_i), (j, y_j), $(0, t)$ pontokon.

K *(Titokmegosztás) Egy széf kódja $m \in \{0, 1, \ldots, p-1\}$, ahol p prím. Egy legföljebb $k-1$-fokú $f(x) \in \mathbb{Z}_p[x]$, m konstans tagú polinomra n résztvevő ($n < p$) közül az i. megkapja az $(i, f(i))$ számpárt ($i = 1, 2, \ldots, n$). Ekkor bármely k résztvevő fel tudja tárni a titkot, de semelyik legföljebb $k-1$ résztvevő nem tud meg semmit a titokról.*