Szegedi Tudományegyetem
Természettudományi és Informatikai Kar
Bolyai Intézet

Alkalmazott matematikus MSc

Záróvizsgatételek

Általános szakirány

Judák Regina
reginajudak@gmail.com

Majernyik Noel
majnol@vipmail.hu

Mezőfi Dávid
david.mezofi93@gmail.com

Utoljára módosítva: 2016. június 14.

Creative Commons licenc

Ez az alkotás a *Creative Commons Nevezd meg! – Ne add el! – Így add tovább! 4.0 Nemzetközi licenc* alá tartozik. A licenc megtekintéséhez látogass el a http://creativecommons.org/licenses/by-nc-sa/4.0/ oldalra.

Tartalomjegyzék

1. Mindkét szakirányon közös tételek

1.1. Gráfelmélet: összefüggőség, színezések

A tételhez kapcsolódó anyagrészek megtalálhatóak Hajnal Péter: *Diszkrét matematika* [4] című kurzusához kapcsolódó honlapon.

Fák összeszámlálása

A [4, *Fokszámsorozatok realizációja* c. részből] érdemes megnézni a gráfok definícióját és a fokszámsorozatok realizációját. A lényeg, hogy akkor realizálható egy fokszámsorozat hurokélmentes gráffal, ha az összegük páros, és egyik elem sem nagyobb mint a többi összege.

Adott fokszámsorozatra speciális esetben megadható, hogy mennyi a fokszámsorozatot realizáló fák száma.

Cayley-tétel. K_n feszítőfáinak a száma n^{n-2} (lásd [4, *Fák összeszámlálása I. – Cayley tétele*]).

Kirchoff-tétel. Tetszőleges irányított gráf feszítőfáinak a száma megadható (lásd [4, *Fák összeszámlálása II. – Kirchoff tétele*, 6. oldal]).

Gráfok élszínezései

Lásd [4, *Gráfok élszínezései*].

A G gráf élszínezése egy $c\colon E(G) \to \mathbb{N}^+$ leképezés. *Jó élszínezés*, ha egy adott csúcson a színek száma megegyezik a fokszámával.

Shannon-tétel. Hurokélmentes gráfban az élkromatikus szám kisebb vagy egyenlő, mint a maximális fokszám másfélszerese.

Vizing-tétel. Egyszerű gráfban az élkromatikus szám kisebb vagy egyenlő, mint a maximális fokszám +1.

Ebben a részben van egy színezési algoritmus, érdekes lehet.

Gráfok csúcsszínezései

Lásd [4, *Gráfok csúcsszínezései I. - tétele*].

A definíció analóg az élekkel, *jó csúcsszínezés*, ha egy adott él két végpontja különböző színű. Három, gráfokon elvégezhető operáció: *bővítés*, *csúcsösszevonás*, *Hajós-operáció*.

G Hajós-konstruálható K_{k+1}-ekből, ha a fenti három operáció elvégzésével véges lépésben megkaphatjuk (nem pontos definíció).

Van 3-4 tétel a k-színezhetőségről az operációkkal kapcsolatosan.

Tétel (Hajós). *G akkor és csak akkor nem k-színezhető, ha Hajós-konstruálható K_{k+1}-ből.*

Derékbőség és kromatikus szám

Lásd [4, *Gráfok csúcsszínezései II.*].

Gráf derékbősége. A gráf legrövidebb körének hossza.

Erdős-tétel. Bármely τ és γ pozitív egészekhez létezik G gráf, melynek a kromatikus száma nagyobb, mint τ és a derékbősége nagyobb, mint γ.

Gráfok magasabb fokú öszefüggősége

Lásd [4, *Folyamok II. – Magasabb fokú összefüggőség*, 18. oldaltól].

k-szorosan élösszefüggő gráf. Bármely k-nál kisebb elemszámú élhalmazt elhagyva a gráf összefüggő marad.

k-szorosan pontösszefüggő gráf. Bármely k-nál kisebb elemszámú csúcshalmazt elhagyva a gráf összefüggő marad.

Menger tételei

Lásd [4, *Folyamok I. – Alaptételek*, 13–16. oldal].

1. Legyen G irányított gráf s, t kitüntett csúcsokkal. Az *éldiszjunkt s–t utak* maximális száma megegyezik azon minimális *élhalmaz* számosságával, melyet ha elhagyunk, nincs s–t út.
2. Ugyanez irányítatlan gráfra.
3. Ugyanez a két tétel pontfüggetlen utakra, lényegében csak az élhalmazt *ponthalmazra*, az éldiszjunkt utat *pontfüggetlen útra* kell cserélni.

1.2. Gráfelmélet: párosítások, síkgráfok

A tételhez kapcsolódó anyagrészek megtalálhatóak Hajnal Péter: *Diszkrét matematika* [4] című kurzusához kapcsolódó honlapon.

Párosítási problémák

Lásd [4, *Párosítások I. – Alapok, nem kombinatorikus módszerek*, 1. szakasz]. Legyen M része a G gráf élhalmazának. Ekkor M *párosítás*, ha M számossága egyenlő $V(M)$ számosságának a felével. *Teljes párosítás*, ha párosítás és $V(M)$ számossága megeggyezik $V(G)$ számosságával.

1. Keressünk maximális párosítást!
2. Határozuk meg a legnagyobb párosítás elemszámát!
3. Döntsük el, van-e a G gráfban teljes párosítás!
4. Keressünk minél nagyobb elemszámú párosítást!

Mohó algoritmus 4-re

Lásd [4, *Párosítások I. – Alapok, nem kombinatorikus módszerek*, 2. szakasz].

Meglévő párosítást adig bővítünk, amíg van olyan él, amit ha hozzáveszünk, párosítás marad. A talált párosítás elemszáma biztosan a maximális párosítás elemszáma és annak a fele között lesz.

Véletlen algoritmus 3-ra (páros gráfok esetén)

Lásd [4, *Párosítások I. – Alapok, nem kombinatorikus módszerek*, 3. szakasz].

Páros gráf szomszédsági mátrixa: olyan, mint a sima szomszédsági mátrix, de itt a sorok az egyik, míg az oszlopok a másik osztályt reprezentálják, ezzel tömörítjük a szomszédsági mátrixot.

Ha M egy párosítás, akkor a páros szomszédsági mátrixban (M-re megszorítva) minden sorban *legfeljebb* 1 darab 1-es van. Teljes párosítás estén *pontosan* 1 darab 1-es. Ez alapján, ha a páros gráf páros szomszédsági mátrixának determinánsa nem 0, akkor létezik teljes párosítás. Legyen X_G az a mátrix amit úgy kapunk, hogy minden e élre az élhez tartozó 1-est x_e-re cseréljük. $\det X_G$ nem azonosan nulla polinom akkor és csak akkor, ha létezik G-ben teljes párosítás.

Ez alapján a véletlen algoritmus: minden x_e-t helyettesítsünk egy uniform véletlen változóval, és számítsuk ki $\det X_G$ értékét. Ha ez 0, akkor `Valószínűleg nem létezik teljes párosítás.` (szerencsétlen eset, ha pont $\det X_G$ gyökeit írtuk be). Ha nem 0, akkor `Biztosan létezik teljes párosítás.`

Javító utas algoritmusok

Lásd [4, *Párosítások II. – Kombinatorikus módszerek*].

$v_0, e_1, \ldots, e_k, v_k$ *javító út* az M párosításra nézve, ha v_0, v_k nem párosítottak, k páratlan, és minden páros indexű él eleme a párosításnak.

Ekkor nagyobb elemszámú párosítást kapunk, ha a javító útból pontosan azokat az éleket vesszük, amik nem voltak benne a párosításban. Ez alapján a javító utas séma: adott M párosítás, keressünk javító utat; ha nem találtunk akkor leállunk, ha találtunk, akkor cseréljük a párosítást az újra, és kezdjük újra az algoritmust.

Berge-tétel. Ha M nem optimális, akkor létezik rá javító út.

Az algoritmusok nehézsége a javító utak keresése.

Mohó algoritmus (címkézés). Lásd [4, *Párosítások II. – Kombinatorikus módszerek*, 2. szakasz].

Magyar módszer. Páros gráf esetén, ha a mohó keresés nem talál javító utat az M párosításra, akkor az M párosítás optimális.

Kőnig-akadály. Csúcsok egy S halmaza *Kőnig-akadály*, ha a szomszédainak száma kisebb mint az elemszáma. Ha egy gráfban van Kőnig-akadály, akkor nincs teljes párosítása.

Edmonds-algoritmus. Lásd [4, *Párosítások II. – Kombinatorikus módszerek*, 3. szakasz].

Tutte-akadály. *Tutte-akadály* a gráf egy olyan ponthalmaza, amelynek elhagyása után a keletkezett páratlan pontszámú komponensek száma több mint az elhagyott pontok száma.

Tutte-tétel. Egy gráf akkor és csak akkor tartalmaz teljes párosítást, ha nincs benne Tutte-akadály.

Síkgráfok

Lásd [4, *Síkgráfok I. – Wagner-tétel*].

Egy gráf *síkgráf*, ha síkbarajzolható. Egy gráf síkbarajzolható, ha le lehet úgy rajzolni, hogy az éleknek csak a végpontokban van közös pontjuk. Szükséges gráfoperációk: él *elhagyása*, élek *összevonása*, él *összehúzása*.

Legyen G gráf.

Részgráf. Ha R a G-ből élek és csúcsok elhagyásával megkapható, akkor R a G *részgráfja*.

Minor. Ha M a G-ből él- és csúcselhagyással, illetve élösszehúzással megkapható, akkor M a G *minorja*.

Topologikus részgráf. Ha T a G-ből él- és csúcselhagyással, illetve élösszevonással megkapható, akkor T a G *topologikus részgráfja*.

Egy részgráf topologikus részgráf is, egy topologikus részgráf minor is egyben. Ha G síkgráf, akkor a részgráfjai, minorjai és topologikus részgráfjai is síkgráfok.

Tétel (Euler). *K_5, és $K_{3,3}$ nem síkgráfok.*

Wagner- és Kuratowski-tétel

Az alábbiak ekvivalensek:

1. G síkgráf;
2. G-nek nem topologikus részgráfja K_5 és $K_{3,3}$;
3. G-ben nincs K_5 és $K_{3,3}$ minor.

Az 1. és 2. pontok ekvivalenciája a Kuratowski-tétel, az 1. és 3. pontok ekvivalenciája a Wagner-tétel.

Metszési szám

Lásd [4, *Síkgráfok II. – Metszési szám és alkalmazásai*].

Egy lerajzolás *reguláris*, ha nincs három élgörbe közös belső ponttal. Gráf *metszési száma*: minimuma azon pontok számának, amelyen több él is átmegy – a minimumot a reguláris lerajzolásokra képezzük.

G síkgráf akkor és csak akkor, ha a metszési száma 0. További két becslés a metszések számára: [4, *Síkgráfok II. – Metszési szám és alkalmazásai*, 4. oldal].

1.3. Gröbner-bázisok és alkalmazásaik

A tételhez kapcsolódó anyagrészek megtalálhatóak Skublics Benedek: *Algoritmuselmélet – Jegyzet Zádori László előadásához* [13] című jegyzetében.

Hilbert bázistétele

Gyűrű alatt kommutatív, egységelemes gyűrűt értünk. Egy adott R gyűrűre $R[\mathbf{x}]$ jelöli az R feletti n határozatlanú polinomgyűrűt.

Egy R gyűrűt *Noether-gyűrűnek* nevezünk, ha minden ideálja végesen generált. Tetszőleges R gyűrű pontosan akkor Noether, ha ideáljaira teljesül a felszálló láncfeltétel, azaz az ideáljai növekvő lánca stabilizálódik (egy idő után az ideálok egyenlőek).

Hilbert bázistétele szerint ha az R gyűrű Noether, akkor $R[x]$ is Noether-gyűrű. Ebből következik, hogy ha K test, akkor $K[\mathbf{x}]$ Noether-gyűrű, illetve $\mathbb{Z}[\mathbf{x}]$ gyűrű Noether.

Hilbert Nullstellensatz

Tétel (Hilbert gyenge Nullstellensatz)**.** *Legyen K algebrailag zárt test. Ha I valódi ideálja $K[\mathbf{x}]$-nek, akkor az I-beli polinomoknak létezik közös zéróhelye K^n-ben.*

Tétel (Hilbert Nullstellensatz)**.** *Legyen K algebrailag zárt test, $H \subseteq K[\mathbf{x}]$ és*

$$V = \{\mathbf{a} \in K^n \mid \forall f \in H\colon f(\mathbf{a}) = 0\}.$$

Ekkor tetszőleges $f \in K[\mathbf{x}]$ polinomra ekvivalensek:

1. *$f(\mathbf{a}) = 0$ minden $\mathbf{a} \in V$ elemre;*
2. *$f^N \in H$ valamely pozitív egész N számra.*

Radikálideálok

Definíció (radikál)**.** Legyen I ideálja az R gyűrűnek. Az alábbi halmazt az I *radikáljának* nevezzük:

$$\sqrt{I} = \{r \in R\colon r^N \in I \text{ valamely pozitív egész } N \text{ számra}\}$$

Definíció (radikálideál)**.** Ha $I = \sqrt{I}$, akkor az I ideált az R *radikálideáljának* nevezzük.

Tétel. *Az R gyűrű tetszőleges I ideálja esetén $\sqrt{I}$ radikálideál.*

Megjegyzés. Tehát a *Hilbert Nullstellensatz* 2. pontja azt jelenti, hogy a H által generált radikálideál tartalmazza az f polinomot.

Galois-kapcsolat, varietások

Csupán egy speciális esetre van szükségünk, amikor adottak A és B halmazok és egy $C \subseteq A \times B$ reláció. Az (α, β) leképezéspárt a C által indukált *Galois-kapcsolatnak* nevezzük, ha

$$\alpha\colon 2^A \to 2^B, \qquad H \mapsto \{b \in B\colon\ (h,b) \in C\ \forall\, h \in H\}$$
$$\beta\colon 2^B \to 2^A, \qquad L \mapsto \{a \in A\colon\ (a,l) \in C\ \forall\, l \in L\}$$

Jelölje (I, V) a C (n-határozatlanú polinom eltűnik **a**-n) által indukált Galois-kapcsolatot. Ekkor a K^n-beli zárt halmazokat *varietásoknak* nevezzük. A Hilbert Nullstellensatz szerint a $K[\mathbf{x}]$-beli zárt halmazok $K[\mathbf{x}]$ radikálideáljai.

Redukciós eljárás

Legyenek $I = (f_1, f_2, \ldots, f_s)$ és $J = (g_1, g_2, \ldots, g_t)$ az R végesen generált ideáljai. A következő kérdésekre szeretnénk választ kapni:

- Van-e olyan algoritmus, amely eldönti tetszőleges $f \in R$ polinom esetén, hogy $f \in I$ vagy $f \notin I$? Ha igen, akkor állítsuk elő az f polinomot az $f_1, f_2, \ldots, f_s$ polinomok R-lineáris kombinációjaként.
- Van-e olyan algoritmus amely eldönti, hogy $I = J$ vagy $I \neq J$?

A két kérdés eldöntése ekvivalens, a kérdések megoldhatóak „szép” bázisok konstruálásával.

Definíció (egylépéses redukált)**.** Legyenek $f, g, h \in K[x_1, x_2, \ldots x_n]$. Jelölje $\hat{g}$ a g polinom legnagyobb (lexikografikus rendezésben) tagját. Ekkor h az f *egylépéses redukáltja* modulo g, ha létezik f-nek olyan $m \neq 0$ tagja, amelynek $\hat{g}$ osztója és $h = f - \left(\frac{m}{\hat{g}}\right) g$.

Definíció (redukált)**.** Legyen $G \subseteq K[x_1, x_2, \ldots x_n]$. Ekkor h az f *redukáltja* modulo G, ha létezik olyan $h_0, h_1, \ldots h_k \in K[x_1, x_2, \ldots x_n]$ sorozat, hogy $h_0 = f$, $h_k = h$ és h_i a h_{i-1} egylépéses redukáltja modulo g, valamely $g \in G$ polinomra.

Ideálok Gröbner-bázisai

Definíció (ideál Gröbner-bázisa)**.** Legyen $G \subseteq K[\mathbf{x}]$ véges polinomhalmaz és I ideálja $K[\mathbf{x}]$-nek. A G halmaz az I *ideál Gröbner-bázisa*, ha $I = (G)$ és minden $f \in I$ nemnulla polinomhoz létezik olyan $g \in G$ polinom, hogy $\hat{g} \mid \hat{f}$.

Definíció (Gröbner-bázis)**.** A G véges polinomhalmazt *Gröbner-bázisnak* nevezzük, ha Gröbner-bázisa a (G) ideálnak.

$$\begin{aligned} G \text{ Gröbner-bázis } &\Leftrightarrow \forall\, f \in (G) \text{ polinom 0-ra redukálható modulo } G \Leftrightarrow \\ &\Leftrightarrow \forall\, f \in K[\mathbf{x}] \text{ polinom teljes redukált alakja egyértelmű} \end{aligned}$$

Ha egy polinom 0-ra redukálható modulo G, akkor az eleme (G)-nek.

Buchberger-algoritmus

Ez előzőek a gyakorlatban nem alkalmasak arra, hogy egy polinomhalmazról eldöntsük, hogy Gröbner-bázis-e. Erre nyújt megoldást a *Buchberger-algoritmus.*

Keressük a (G) ideál Gröbner-bázisát.

1: $f, g \in G$ kiválasztása.
2: $s(f, g)$ kiszámolása. ▷ s-polinom.
3: $s(f, g)$ redukálása, ameddig lehet.

4: $h \leftarrow$ az így kapott teljes redukált
5: **if** $h = 0$ **then**
6: Újra az elejétől.
7: **else**
8: Vegyük hozzá h-t G-hez és ismételjük az elejétől.

Ez az eljárás véges számú lépés után véget ér, és a kapott halmaz a (G) Gröbner-bázisa.

Minimális és redukált Gröbner-bázisok

Egy Gröbner-bázis *minimális*, ha nem eleme a 0 és a különböző elemeinek legnagyobb tagja nem osztja egymást. Egy Gröbner-bázis *teljesen redukált*, ha nem eleme a 0 és egyik g tagja sem redukálható tovább modulo $G \setminus \{g\}$.

Tartalmazási problémák

Ideál tartalmazási probléma. Határozzuk meg, hogy adott $f \in K[\mathbf{x}]$ polinomra és $F \subseteq K[\mathbf{x}]$ véges polinomhalmazra teljesül-e $f \in (F)$! Megoldás a Buchberger-algoritmussal.

Radikál tartalmazási probléma. Határozzuk meg, hogy adott $f \in K[\mathbf{x}]$ polinomra és $F \subseteq K[\mathbf{x}]$ véges polinomhalmazra teljesül-e $f \in \sqrt{(F)}$! Megoldás egy tétel és az előző feladat megoldására alkalmazott algoritmus segítségével.

Algebrailag zárt test feletti egyenletrendszerek megoldhatósága

Határozzuk meg, hogy $f_1, f_2, \ldots, f_k \in K[\mathbf{x}]$ polinomokra van-e megoldása az $f_1 = 0, f_2 = 0, \ldots, f_k = 0$ egyenletrendszernek!

Megoldás Gröbner-bázissal: ha van a bázisban konstans, megoldható, különben nem.

Gráfszínezési probléma

Gráfok kétszínezhetőségére ismert hatékony algoritmus, azonban a háromszínezhetőség eldöntése NP-teljes probléma. A Buchberger-algoritmussal azonban eldönthető, hogy egy gráf háromszínezhető-e. A problémát ehhez vissza kell vezetni az egyenletrendszer megoldhatóságának problémájára.

Minimálpolinom-keresés

Legyen adott a $K(\alpha) \mid K$ egyszerű algebrai testbővítés, és tegyük fel, hogy ismerjük α minimálpolinomját. A Buchberger-algoritmus segítségével meghatározható egy adott $\beta \in K(\alpha)$ elem minimálpolinomja.

1.4. Matematikai titkosírások

A tételhez kapcsolódó anyagrészek megtalálhatóak Skublics Benedek: *Algoritmuselmélet – Jegyzet Zádori László előadásához* [13] című jegyzetében.

Alapfogalmak és célok

A *kriptológia* a titkosírás tudománya, melynek két fő ága van.

Kriptográfia. Titkosírási rendszerek *tervezése*.

Kriptoanalízis. Titkosírási rendszerek *megfejtése*.

A kriptográfia alapfeladata annak a problémának a megoldása, hogy két pont között úgy tudjunk titkos üzenetet küldeni, hogy a küldés során az üzenet mindvégig titkos maradjon. Erre az *alapeljárás* a következő: A és B szeretne titkos üzenetet váltani, mely üzenet legyen x. Ehhez szükségük van egy-egy titkos kulcsra, legyenek ezek: a és b. Szükséges továbbá egy E kódoló és egy D dekódoló függvény. A kódolt üzenete $E(x, a)$, melyet elküld B-nek, aki dekódolja: $D(E(x, a), b) = x$, így visszakapva az eredeti x üzenetet.

Nyilvános kulcsú titkosírás

Az alapfeladat megoldására több lehetőségünk is van, az egyik ilyen a *nyilvános kulcsú titkosírások*. A nyilvános kulcsú titkosírásokkal bizonyos feltételek mellett az is ellenőrizhető, hogy az üzenetet ki küldte (hitelesítés, autentikáció).

Az alapelv a következő: adott felhasználók egy $\{F_1, F_2, \ldots, F_n\}$ halmaza, mindenkinek rendelkeznie kell egy k_i nyilvános és egy l_i titkos kulccsal. Egy f függvényt *kódoló és dekódoló függvénynek* nevezünk, ha teljesülnek az alábbiak:

1. $f\left(f\left(x, k_i\right), l_i\right) = x$ minden x üzenetre és indexre;
2. x és y ismeretében $f\left(x, y\right)$ gyorsan számolható;
3. y és $f\left(x, y\right)$ ismeretében x nem számolható gyorsan;
4. ha $f\left(f\left(x, l_i\right), k_i\right) = x$ is teljesül minden x üzenetre és indexre, akkor hitelesíteni is tudjuk az üzenet küldőjét.

Ekkor az eljárás a következő: tegyük fel,hogy F_1 küld üzenetet F_2-nek. F_1 az $f\left(x, k_2\right)$-t küldi el F_2-nek, aki ezután kiszámolja $f\left(f\left(x, k_2\right), l_2\right) = x$-et.

Ha a 4. feltétel is teljesül, akkor F_1 az $f\left(f\left(x, l_1\right), k_2\right)$-t küldi el F_2-nek, aki az $f\left(f\left(f\left(f\left(x, l_1\right), k_2\right), l_2\right), k_1\right)$-et számolja ki.

RSA

Minden F_i felhasználó a következőeket teszi:

- választ két nagy prímet: p_i, q_i;
- kiszámolja a szorzatuk: $m_i = p_i q_i$;
- k_i szám választása úgy, hogy $1 < k_i < \varphi\left(m_i\right)$ és $\operatorname{lnko}\left(k_i, \varphi\left(m_i\right)\right) = 1$;
- l_i kiszámolása: $1 < l_i < \varphi\left(m_i\right)$ és $k_i l_i \equiv 1 \mod \varphi\left(m_i\right)$;
- *nyilvános kulcs*: (k_i, m_i);
- *titkos kulcs*: (l_i, m_i).

Az $f\left(x, (y, z)\right)$ kódolófüggvény az $(x, (y, z))$ párhoz az x^y legkisebb nemnegatív maradékát rendeli modulo z (feltesszük, hogy az x üzenetre teljesül: $0 \leq x < \min_i m_i$).

Prímtesztek

A prímszámok fontos szerepet játszanak a titkosírás során, tehát szükségünk van olyan eljárásokra, melyekkel tesztelni tudjuk egy számról, hogy prím vagy összetett szám-e. A kis Fermat-tétel egy szükséges feltételt ad arra, hogy egy szám prímszám-e, a feltétel azonban nem fordítható meg.

Soloway – Strassen. A jegyzetben nem szerepel, algoritmuselmélet gyakorlaton volt róla szó.

Bemenet: n és k számok

1: **for** $i \leftarrow 1, i < k, i \leftarrow i + 1$ **do**
2: $\quad a \leftarrow \textsc{Random}(0, n-1)$
3: $\quad x \leftarrow a^{\frac{n-1}{2}} \mod n$
4: $\quad y \leftarrow \left(\frac{a}{n}\right) \mod n$
5: $\quad$ **if** $x \neq y$ **then**
6: $\quad\quad$ **return** n `nem prím`
7: **return** n `valószínűleg prím`

Ha n prím, akkor az output *mindig* n `valószínűleg prím` lesz, ha n összetett, akkor az output $1 - 2^{-k}$ valószínűséggel n `nem prím`. Az x és y értékeknek az *Euler-lemma* értelmében kell egyenlőnek lenniük feltéve, hogy n prím. Az $\left(\frac{a}{n}\right)$ érték a *Jacobi-szimbólum.*

Miller – Rabin. A Miller – Rabin-prímteszt egy egyszerű számelméleti észrevételen alapuló nemdeterminisztikus prímteszt. Elvégzésével csupán nagy valószínűséggel állíthatjuk, hogy a tesztelt szám prímszám. A tesztelés determinisztikussá tehető az általánosított Riemann-hipotézis segítségével.

Legyen n a tesztelendő páratlan szám, $n = 2^k r + 1$, r páratlan. Legyen $0 < a < n$. Ha n prímszám, akkor az alábbi állítás minden a-re teljesül, ha n összetett, akkor ez legfeljebb $\frac{n+1}{2}$ db a számra igaz:

$$a^r \equiv 1 \mod n \text{ vagy van olyan } 0 \leq i < k, \text{ hogy } a^{2^i r} \equiv -1 \mod n.$$

Ezért véletlenszerűen választunk a értékeket, és ha mondjuk 100 egymás utáni választásra igaz a fenti állítás, akkor n nagy valószínűséggel prím. Ha t-szer ismétlünk, akkor legfeljebb $\frac{1}{2^t}$ a valószínűsége annak, hogy egy összetett számot prímnek nyilvánítunk.

AKS. Ez az első determinisztikus polinomiális futási idejű prímteszt, 2002-ből való és három indiai matematikus nevéhez kötődik: *Agraval*, *Kayal* és *Saxena.* A gyakorlatban inkább a Miller – Rabint alkamazzák (gyorsabb, bár futásideje elméletileg nem polinomiális).

Legyen $n \geq 2$ természetes szám, r olyan n-nél kisebb természetes szám, hogy n rendje modulo r nagyobb, mint $\log_{10}^2 n$. Az n szám pontosan akkor prím, ha:

1. n nem teljes hatvány;
2. n-nek nincs prímtényezője, ami $\leq r$;
3. $(x + a)^n \equiv x^n + a \mod (n, x^r - 1)$ teljesül minden $1 \leq a \leq r$ egész számra.

A diszkrét logaritmus és alkalmazásai

Definíció. Legyen G egy véges ciklikus csoport, $g \in G$ egy generátorelem és $a \in G$ egy tetszőleges elem. Ekkor az a elem g alapú *indexe/diszkrét logaritmusa* az a legkisebb nemnegatív egész k szám, amelyre $a = g^k$, jelölésben $\operatorname{ind}_g a$.

A diszkrét logaritmus kiszámítására nem ismert hatékony algoritmus, még akkor sem, ha ciklikus csoportok helyett csak a $\mathbb{Z}_p^*$ alakú csoportokra szorítkozunk. Ezt a problémát használja ki a következő két algoritmus.

Diffie – Hellman-kulcsváltás. Az eljárás a diszkrét logaritmus problémáján alapszik. Az eljárás célja, hogy két felhasználó számára egy közös titkos kulcsot hozzon létre nyilvános kommunikációs csatornán keresztül.

Massey – Omura-rejtjelrendszer. Ez az eljárás is a diszkrét logaritmus problémáján alapszik, segítségével a felek biztonságosan tudnak titkos üzenetet küldeni egymásnak.

Dióhéjban: elküldök egy ládát lelakatolva B-nek, ő is ráteszi a saját lakatját, és visszaküldi nekem, én leveszem a saját lakatomat, és visszaküldöm B-nek, aki így már ki tudja nyitni a ládát.

1.5. Többváltozós és vektorértékű függvények

A tételt próbáltam egy kicsit szemléletes oldalról is megközelíteni, amihez a Wikipedia nyújtott se- JR

gítséget. A precízebb definíciók és tételek az órai jegyzetek és a *Thomas-féle kalkulus* III. része [14, 16. fejezet] alapján születtek meg. Nem minden dolog szerepel ugyanilyen módon a Thomas-könyvben, azonban vizsga előtti felkészüléshez egy nagyon jó alap lehet, mert a tétel majdnem minden részét lefedi, és könnyen megtalálhatóak benne a dolgok.

Többszörös integrál

Integrálni nem csak intervallumok felett lehet. Általánosan, egy adott E halmaz fölötti integrált a következőképpen jelölünk:

$$\int_E f(\mathbf{x}) \, \mathrm{d}\mathbf{x}.$$

Itt $\mathbf{x}$-nek nem muszáj valós változónak lennie, lehet például $\mathbb{R}^3$-beli vektorértékű változó is. A *Fubini-tétel* szerint az ilyen integrálok felírhatóak integrálok integráljaként. Tehát az ilyen „területek" vagy „térfogatok" feletti integrálok kiszámítható az egyes koordináták szerinti egyenkénti integrálással.

Ahogy a pozitív egyváltozós függvények határozott integrálja a függvény és az x-tengely által bezárt területet adja meg, úgy a kettős integrálja egy pozitív kétváltozós függvénynek megadja az integrálási tartomány és a függvény által meghatározott felület által bezárt térfogatot. Ugyanezt térfogatot kiszámíthatjuk hármas integrállal is. Ekkor a hármas integrál teljes integrálási tartománya a fent említett tartomány, amit a függvény és a kettős integrál integrálási tartománya bezár – tehát az egész közrezárt térrész, térfogat – míg az integrandus a konstans 1 függvény. Ha a változók száma és az integrálok száma nagyobb, akkor a kifejezés az adott dimenziós térfogatnak felel meg.

Tétel. *Legyen $R = [a,b] \times [c,d]$ véges vagy nem véges téglalap az $\mathbb{R}^2$ térben. Az R téglalapon értelmezett, integrálható f függvény integrálja kiszámítható az egyes változók szerint való szukcesszív integrálással:*

$$\iint_R f(x,y) \, \mathrm{d}x \, \mathrm{d}y = \int_a^b \int_c^d f(x,y) \, \mathrm{d}y \, \mathrm{d}x = \int_c^d \int_a^b f(x,y) \, \mathrm{d}x \, \mathrm{d}y.$$

Vonalintegrál és fizikai alkalmazásai

Az integrálás elve kiterjeszthető általánosabb alaphalmazokra is, mint például adott görbék menti integrálásra vagy felületek feletti integrálásra. Ezen típusú integrálok a fizika fontos eszközei (különféle vektormezőkkel kapcsolatosan).

A *vonalintegrál* olyan integrál, aminek az integrandusát egy adott görbe mentén integráljuk. Ha az adott görbe zárt görbe, vagyis ha a kezdő és a végpontja megegyezik akkor a vonalintegrál *körintegrál*.

A vonalintegrál integrandusa lehet skalárértékű vagy vektorértékű is. A *vonalintegrál értéke* az adott görbe mentén előforduló elemek súlyozott összege. A súlyozást úgy kell érteni, hogy a görbét „lépésekre" bontjuk, vagyis kijelölünk rajta pontokat, amely pontokban vesszük az integrandus értékét és megszorozzuk az előző és az aktuális pont közötti távolsággal. Ha az integrandus nem skalár-, hanem vektorértékű, akkor a görbe adott pontbeli lineáris közelítésével, érintővektorával, való skaláris szorzatát vesszük. Az így kapott szorzatokat összegezzük. Ha minden pont közötti görberésznek a hossza a 0-ba tart akkor kapjuk meg a vonalintegrál pontos értékét.

Mindez precízebben:

Skalárfüggvény görbe menti vonalintegrálja.

- Legyen $G \subset \mathbb{R}^3$ egy nyílt és ívszerűen összefüggő tartomány, továbbá $f\colon G \to \mathbb{R}$ folytonos függvény.
- Legyen C egy görbe G-ben: $\mathbf{r}\colon [a,b] \to G$ folytonos, szakaszonként sima.
- A görbe ívhossza: $s(t) = \int_a^t |\mathbf{r}'(\tau)| \, \mathrm{d}\tau$.
- Legyen $\mathbb{B}$ egy beosztása az $[a,b]$ intervallumnak: $a = t_0 < t_1 < \ldots < t_n = b$ és $t_k^* \in \in [t_{k-1}, t_k]$.

– Tekintsük az integrálközelítő összeget:

$$S_{\mathbb{B}} = \sum_{k=1}^{n} f\left(\mathbf{r}\left(t_k^*\right)\right)\left(s\left(t_k\right) - s\left(t_{k-1}\right)\right) \to I$$

ha $\mathbb{B}$ finomsága 0-hoz tart, ahol

$$I = \int_C f \,\mathrm{d}s = \int_a^b f\left(\mathbf{r}\left(t\right)\right)\left|\mathbf{r}'\left(t\right)\right| \,\mathrm{d}t \qquad \left(\mathrm{d}s = s'\left(t\right)\mathrm{d}t = \left|\mathbf{r}'\left(t\right)\right|\mathrm{d}t\right)$$

az f *skalárfüggvény* C *görbe menti vonalintegrálja.*

Vektormező görbe menti vonalintegrálja.

– Legyen $G \subset \mathbb{R}^3$ egy nyílt és ívszerűen összefüggő tartomány, továbbá $\mathbf{F}\colon G \to \mathbb{R}^3$ folytonos leképezés, melyet *vektormezőnek* nevezünk:

$$(x,y,z) = \mathbf{x} \mapsto \mathbf{F}\left(\mathbf{x}\right) = P\left(x,y,z\right)\mathbf{i} + Q\left(x,y,z\right)\mathbf{j} + R\left(x,y,z\right)\mathbf{k}.$$

– $\mathbf{T}\left(t\right) = \frac{\mathbf{r}'(t)}{|\mathbf{r}'(t)|}$ az érintő irányú egységvektor.

– Az $\mathbf{F}$ *vektormező* C *görbe menti vonalintegrálja*:

$$\int_C \mathbf{F}\cdot\mathbf{T}\,\mathrm{d}s = \int_a^b \mathbf{F}\left(\mathbf{r}\left(t\right)\right)\frac{\mathbf{r}'\left(t\right)}{\left|\mathbf{r}'\left(t\right)\right|}\left|\mathbf{r}'\left(t\right)\right| \,\mathrm{d}t = \int_a^b \mathbf{F}\left(\mathbf{r}\left(t\right)\right)\cdot\mathbf{r}'\left(t\right) \,\mathrm{d}t =$$
$$= \int_C \mathbf{F}\cdot\mathrm{d}\mathbf{r} = \int_a^b P\,\mathrm{d}x + Q\,\mathrm{d}y + R\,\mathrm{d}z.$$

A fizika számos részén használható az így definiált vonalintegrál. Például egy erőtér egy részecskén végzett munkáját kiszámíthatjuk a vonalintegrál segítségével. A munka alapesetben, ha az erő állandó az elmozdulás pedig egyenes akkor kiszámítható a $W = \mathbf{F}\cdot\mathbf{s}$ képlettel. Ha azonban a részecske egy adott C görbe mentén mozog a térben, az adott pontban ráható erőt (amely egy vektor) az $\mathbf{F}$ vektormező adja meg akkor az *erőtér* (a vektormező) által a részecskén végzett munka általánosan megkapható úgy, hogy az utat „infinitezimális" részekre bontjuk, amelyeket egyenesnek veszünk. Ekkor a teljes munka megegyezik ezen részutakon végzett munkák összegével, így kapjuk a

$$W = \int_C \mathbf{F}\cdot\mathrm{d}\mathbf{r}$$

vonalintegrált. Ha $\mathbf{F}$ egy *áramlási mező*, azaz pl. egy áramló folyadék sebességvektormezője, akkor az *áramlás* $\int_C \mathbf{F}\cdot\mathrm{d}\mathbf{r}$. Ha a görbe zárt, ez a görbe menti *cirkuláció*.

Ha az x–y-sík egy zárt görbével határolt részét tekintjük, és azt akarjuk kiszámolni, hogy milyen gyorsan áramlik be ide vagy innen ki a folyadék, akkor az $\mathbf{F}\cdot\mathbf{n}$ skalár kifejezést kell integrálnunk a C görbe mentén. Itt az $\mathbf{n}$ a görbére merőleges, „kifelé mutató" egységvektor, és $\mathbf{F}\cdot\mathbf{n}$ az áramlási mező $\mathbf{n}$ irányú komponense. Ez az integrál $\mathbf{F}$ *fluxusa* a C görbén:

$$\oint_C \mathbf{F}\cdot\mathbf{n}\,\mathrm{d}s = \int_a^b P\,\mathrm{d}y - Q\,\mathrm{d}x.$$

Felületi integrál

A *felületi integrál* olyan határozott integrál, amelynek integrálási tartománya egy felület. Az előzőek szerint ez felírható mint egy többszörös integrál. Az integrandus lehet skalárértékű vagy vektorértékű is. Az adott felületet felbonthatjuk kisebb részekre és ezeken a felosztásokon egy Riemann-összeghez

hasonló összeget definiálhatunk. A felületi integrál ennek az összegnek a határértéke, ahogy a felosztás minden elemének a mértéke 0-ba tart.

Például legyen adott egy $\mathbf{V}$ vektormező és egy S felület a térben, vagyis minden $\mathbf{x} \in S$-re, $\mathbf{V}(\mathbf{x})$ egy vektor. Képzeljük el, hogy egy folyadék keresztülfolyik az S felületen úgy, hogy minden $\mathbf{x}$ pontjában az S felületnek a folyadék sebessége $\mathbf{V}(\mathbf{x})$. A *fluxus* azt adja meg, hogy egy adott felületen egységnyi idő alatt mennyi folyadék áramlik át. A fluxus kiszámításához S minden pontjában vennünk kell a folyadék áramlási sebességének és a felület (adott pontbeli) normálisának a skaláris szorzatát. Ez meghatároz egy skalárteret S minden pontjában, amelyet a felületen integrálva kapjuk, hogy

$$\iint_S \mathbf{V} \cdot \mathrm{d}\mathbf{S}.$$

Az ilyen típusú integrálok jelentik az alapját például az elektrodinamikának.

Felszín kiszámítása.

- Legyen D egy paramétertartomány az u–v-síkban.
- Az S felület folytonos paraméterezése: $\mathbf{r}\colon D \to \mathbb{R}^3$.
- S sima, azaz $\mathbf{r}$ folytonosan differenciálható u és v szerint és $\mathbf{r}'_u \times \mathbf{r}'_v \neq 0$ (egyik sem nulla és nem párhuzamosak).
- Az érintősík egységnyi hosszúságú normálvektora: $\mathbf{n} = \frac{\mathbf{r}'_u \times \mathbf{r}'_v}{|\mathbf{r}'_u \times \mathbf{r}'_v|}$.
- Ha felbontjuk kis területdarabokra a paramétertartományt, akkor minden darabka felett egy felületdarab fekszik, melyek területe közelítőleg egyenlő az érintővektorok által kifeszített paralelogramma területével.
- A teljes felszín közelítőleg egyenlő ezen paralelogrammák területének összegével:

$$\hat{A}(S) = \sum_{k,\ell} A(S_{k,\ell}) = \sum_{k,\ell} \left|\mathbf{r}'_{u_k} \times \mathbf{r}'_{v_\ell}\right|,$$

  és ha a beosztás finomsága nullához tart, akkor

$$\hat{A}(S) \to A(S) = \iint_D \left|\mathbf{r}'_u \times \mathbf{r}'_v\right| \,\mathrm{d}u\,\mathrm{d}v.$$

Felszín szerinti integrál.

- Az $f(x,y,z)$ skalárfüggvény felszín szerinti integrálja:

$$\iint_S f(x,y,z)\,\mathrm{d}S = \iint_D f(\mathbf{r}(u,v)) \left|\mathbf{r}'_u \times \mathbf{r}'_v\right| \,\mathrm{d}u\,\mathrm{d}v.$$

- Az $\mathbf{F}(x,y,z)$ vektorfüggvény felszín szerinti integrálja:

$$\iint_S \mathbf{F}(x,y,z)\,\mathrm{d}\mathbf{S} = \iint_D \mathbf{F}(\mathbf{r}(u,v)) \cdot \left(\mathbf{r}'_u \times \mathbf{r}'_v\right) \,\mathrm{d}u\,\mathrm{d}v = \iint_S \mathbf{F} \cdot \mathbf{n}\,\mathrm{d}S$$

Green-, Gauss-, Stokes-tétel

Definíció (rotáció, divergencia)**.** Legyen $\mathbf{F}(\mathbf{x}) = P(x,y,z)\,\mathbf{i} + Q(x,y,z)\,\mathbf{j} + R(x,y,z)\,\mathbf{k}$ vektorfüggvény. Ekkor $\mathbf{F}$ *rotációját* és *divergenciáját* a következőképp definiáljuk:

$$\operatorname{rot}\mathbf{F} = \left(R'_y - Q'_z, P'_z - R'_x, Q'_x - P'_y\right) \qquad \text{(vektorfüggvény)}$$

$$\operatorname{div}\mathbf{F} = P'_x + Q'_y + R'_z \qquad \text{(skalárfüggvény)}$$

Tétel (Green). *Legyen C egy pozitív irányítású szakaszonként sima, egyszerű, zárt görbe, mely a D tartomány határa. Legyen továbbá $\mathbf{F}\colon D \to \mathbb{R}^2$ egy vektormező, $\mathbf{F} = P(x,y)\,\mathbf{i} + Q(x,y)\,\mathbf{j}$. Ekkor*

$$\oint_C \mathbf{F}\cdot \mathrm{d}\mathbf{r} = \int_C P\,\mathrm{d}x + Q\,\mathrm{d}y = \iint_D \left(Q'_x - P'_y\right)\,\mathrm{d}x\mathrm{d}y.$$

Tétel (Gauss). *Legyen V egy egyszeresen összefüggő térfogat, melynek határa az S felület (szakaszonként sima). Legyen $\mathbf{F}$ egy folytonosan differenciálható vektorfüggvény. Ekkor*

$$\iiint_V \operatorname{div}\mathbf{F}\,\mathrm{d}V = \iint_S \mathbf{F}\cdot\mathrm{d}\mathbf{S}.$$

Tétel (Stokes). *Legyen S egy felszíndarab, melynek a határa C, ami egy zárt görbe. Legyen $\mathbf{F}$ egy folytonosan differenciálható vektorfüggvény. Ekkor*

$$\iint_S \operatorname{rot}\mathbf{F}\cdot\mathrm{d}\mathbf{S} = \oint_C \mathbf{F}\cdot\mathrm{d}\mathbf{r}.$$

1.6. Fourier-sorok, ortogonális polinomok, sorfejtések

A tételhez kapcsolódó anyagrészek megtalálhatóak Németh Zoltán és Szabó Tamás *Alkalmazott analízis* című tárgyhoz készült jegyzetében [10].

Trigonometrikus és ortogonális polinomsorok konvergenciája

Lásd [10, 1.3. és 1.6. szakaszok]. Érdemes lehet átolvasni [10, 1.4. és 1.5. szakaszokat] is.

Legyen V egy skaláris szorzatos, teljes vektortér, (ϕ_n) egy ortogonális rendszer és $f \in V$ rögzített. Ha $c_n = \langle f, \phi_n\rangle$, akkor az f *általános Fourier-sora* a következő:

$$f \sim \sum c_n\phi_n.$$

A továbbiakban a valós egyenesen értelmezett, 2π-periodikus függvényekkel foglalkozunk.

Jelölje $\mathbb{T}$ az $\mathbb{R}/2\pi\mathbb{Z}$ faktorcsoportot ($2\pi\mathbb{Z}$ a $2k\pi$ alakú számok additív csoportja). Legyen $f \in L^1(\mathbb{T})$, ahol az f függvény *Fourier-sora* a következő:

$$f \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n\cos nx + b_n\sin nx, \quad \text{ahol} \quad \begin{cases} a_n = \dfrac{1}{\pi}\displaystyle\int_{-\pi}^{\pi} f(t)\cos nt\,\mathrm{d}t & (n\in\mathbb{N}_0)\,; \\ b_n = \dfrac{1}{\pi}\displaystyle\int_{-\pi}^{\pi} f(t)\sin nt\,\mathrm{d}t & (n\in\mathbb{N})\,. \end{cases}$$

Páros függvény esetén $b_n = 0$, míg páratlan függvény esetében $a_n = 0$ minden n-re. Minden Fourier-sor egyben trigonometrikus sor is.

Az f függvény *Fourier-sorának komplex alakja* a következő:

$$f \sim \sum_{k=-\infty}^{\infty} \hat{f}(k)\,\mathrm{e}^{\mathrm{i}kx}, \quad \text{ahol} \quad \hat{f}(k) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t)\,\mathrm{e}^{-\mathrm{i}kt}\,\mathrm{d}t \quad (k\in\mathbb{Z})\,.$$

A sor n-ik részletösszege:

$$s_n(x) = \sum_{k=-n}^{n} \hat{f}(k)\,\mathrm{e}^{\mathrm{i}kx}.$$

Az $(1, \cos t, \sin t, \cos 2t, \sin 2t, \ldots)$ rendszer *ortogonális*, a $\phi_k(t) = \mathrm{e}^{-\mathrm{i}kt}$ $(k\in\mathbb{Z})$ függvények pedig *ortonormált* rendszert alkotnak.

Kérdés. Mikor állítja elő egy függvény Fourier-sora a függvényt? Pontonkénti konvergenciát vizsgálunk, azaz arra vagyunk kíváncsiak, hogy egy adott x pontban konvergens-e az alábbi sor:

$$\sum_{k=-\infty}^{\infty} \hat{f}(k)\, \mathrm{e}^{\mathrm{i}kx}?$$

- Ha a függvény L^2-beli, akkor Fourier-sora a függvényhez az L^2 tér normájában konvergens.
- $s_n(x)$ felírható a Dirichlet-mag felhasználásával, aminek segítségével belátható, hogy ha egy függvény L^1-beli és teljesül rá a Dini-feltétel, akkor a Fourier-sor x-ben a függvényértékhez konvergál.
- Ha α-rendű Lipschitz-feltétel teljesül a függvényre x-ben, akkor ott folytonos is. Ha f az x-ben differenciálható, akkor 1-rendű Lipschitz teljesül. Továbbá a Lipschitz-feltételből következik, hogy teljesül a Dini-feltétel is.
- Ha f L^1-beli és folytonos x-ben és ott $0 < \alpha \leq 1$-rendű Lipschitz-feltétel teljesül rá, vagy pedig x-ben differenciálható, akkor a Fourier-sor x-ben a függvényértékhez konvergál.
- Ha az f függvény nem folytonos, de az x szakadási helyen léteznek a féloldali határértékek, és a féloldali Dini-feltétel teljesül rá vagy pedig mindkét oldalon teljesül a Lipschitz-feltétel vagy mindkét oldalon féloldalról differenciálható, akkor a Fourier-sor x-ben a féloldali határértékek átlagához konvergál.

Fourier-transzformált

Lásd [10, 4.1. és 4.5. szakaszok].

A Fourier-sor definíciója megfogalmazható $2p$ periodikus függvényekre is. Hasonló előállítás adható nem periodikus függvények esetére is. Az alapötlet az, hogy $p \to \infty$ határátmenettel a $2p$ periodikus függvényből megkapjuk az egész számegyenesen értelmezett függvény esetét, amivel megkaphatjuk a Fourier-sorfejtés formuláinak folytonos analogonjait.

Legyen $f \in L^1(\mathbb{R})$. Az f *Fourier-transzformáltja* a következő függvény:

$$\mathcal{F}f(\omega) = \hat{f}(\omega) = \int_{-\infty}^{\infty} f(t)\, \mathrm{e}^{-\mathrm{i}\omega t}\, \mathrm{d}t \qquad (\omega \in \mathbb{R}).$$

Ez a definíció korrekt, hiszen $\left|\mathrm{e}^{-\mathrm{i}\omega t}\right| = 1$.

Az *inverziós formula* a következő:

$$f(t) \sim \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{f}(\omega)\, \mathrm{e}^{\mathrm{i}\omega t}\, \mathrm{d}\omega.$$

Ha f az t-ben olyan, hogy

$$\int_{-\delta}^{\delta} \left| \frac{f(t+u) + f(t-u)}{2u} \right| \mathrm{d}u < \infty, \quad \text{akkor} \quad f(t) = \lim_{R\to\infty} \frac{1}{2\pi} \int_{-R}^{R} \hat{f}(\omega)\, \mathrm{e}^{\mathrm{i}\omega t}\, \mathrm{d}\omega.$$

Laplace-transzformált

Lásd [10, 6.1–6.4 szakaszok].

Legyen f a valós t idő változónak valós/komplex értékű függvénye, továbbá legyen s egy rögzített valós/komplex szám. Az $f(t)$ függvény *Laplace-transzformáltja* a következő függvény:

$$F(s) = L[f(t)](s) = \int_0^{\infty} f(t)\, \mathrm{e}^{-st}\, \mathrm{d}t = \lim_{b\to\infty} \int_0^{b} f(t)\, \mathrm{e}^{-st}\, \mathrm{d}t,$$

amennyiben az improprius integrál létezzik s-ben.

Ha az $f(t)$ függvény Laplace-transzformáltja $F(s)$, akkor $F(s)$ inverz Laplace-transzformáltja $f(t)$. Az inverz Laplace-transzformált a folytonos függvények körében egyértelmű és ebből kifolyólag inverz Laplace-transzformálton általában folytonos függvényt értünk.

1.7. Közönséges differenciálegyenletek és elsőrendű parciális differenciálegyenletek

A tételhez kapcsolódó anyagrészek egy része megtalálható a *Differential Equations, Dynamical Systems and an Introduction to Chaos* [6] című könyvben.

Közönséges. Az ismeretlen függvény egyváltozós.

Parciális. Az ismeretlen függvény többváltozós.

Az f függvény *Lipschitz-folytonos* valamely Ω halmazon, ha létezik L valós szám, hogy bármely $x, y \in \Omega$ esetén $|f(x) - f(y)| < L|x - y|$.

Ha egy függvény differenciálható, akkor Lipschitz-folytonos; ha Lipschitz-folytonos, akkor folytonos.

$$\begin{aligned} u'(t) &= f(t, u(t)); \\ u(t_0) &= u_0. \end{aligned} \tag{KÉP}$$

Picard – Lindelöf-tétel

Ha f folytonos az első változójában és Lipschitz a másodikban, akkor létezik a kezdetiérték problémának megoldása és a megoldás egyértelmű.

Azt a pontot ahol az egyenlet jobb oldala nulla, *egyensúlyi helyzetnek* nevezzük. Az u_0 egyensúlyi helyzet *stabil*, ha bármely pozitív ϵ-hoz epszilonhoz létezik pozitív δ úgy, hogy ha $|x - u_0| < \delta$, akkor $|u(t; x) - u_0| < \epsilon$ (lásd [6, 175. oldal]). *Instabil*, ha nem stabil. *Asszimptotikusan stabil*, ha stabil és létezik olyan σ, hogy ha $|x - u_0| < \sigma$, akkor $u(t; x)$ tart u_0-hoz.

Megmaradási törvények

Polner-féle jegyzet 70. diától.

Alakja: $u_t + c(u)\, u_x = 0$. Megoldás: karakterisztikus görbék, a megoldás konstans a karakterisztikus görbék mentén, megoldása a kezdeti érték problémának. Megoldás $f(x - c(f(x))\, t)$.

Esetleg érdemes megnézni mi van, ha a karakterisztikák metszik egymást, és a gyenge megoldások definícióját (83. dia).

Numerikus algoritmusok és CFL-feltétel a módszer stabilitására: 97–101 dia.

1.8. Többdimenziós normális eloszlású vektorok statisztikai analízise

A tételhez kapcsolódó anyagrészek megtalálhatóak a Bolla Marianna – Krámli András: *Statisztikai következtetések elmélete* [2] című könyvben.

Definíció (p-dimenziós standard normális eloszlás)**.** Az $\mathbf{Y}$ véletlen vektor *p-dimenziós standard normális eloszlású* – jelölésben $\mathbf{Y} \sim \mathcal{N}_p(\mathbf{0}, \mathbf{I}_p)$ –, ha komponensei egydimenziós standard normális eloszlásúak és függetlenek.

Ha $\det \mathbf{A} \neq 0$ és $\mathbf{X} = \mathbf{AY} + \mathbf{m}$, akkor $\mathbf{X} \sim \mathcal{N}_p(\mathbf{m}, \mathbf{C})$, ahol $\mathbf{C} = \mathbf{AA}^{\mathrm{T}}$ ($\mathbf{C}$ szimmetrikus és pozitív definit, mivel *Gram-mátrix* és $\mathbf{A}$ nemszinguláris).

Wishart-eloszlás

Wishart-mátrix. A $p\times p$-s $\mathbf{W}$ véletlen mátrixot *p-dimenziós, n szabadságfokú* $\mathbf{C}$ kovarianciamátrixú (centrális) *Wishart-mátrixnak* nevezzük, ha előállítható $\mathbf{W}=\mathbf{X}\mathbf{X}^{\mathrm{T}}$ alakban, ahol a $p\times n$-es $\mathbf{X}$ véletlen mátrix oszlopvektorai függetlenek és $\mathcal{N}_p(\mathbf{0},\mathbf{C})$ eloszlásúak.

Wishart-eloszlás. Ilyen mátrix elemeinek együttes eloszlását $(p,n,\mathbf{C})$ paraméterű (centrális) *Wishart-eloszlásnak* nevezzük – jelölésben $\mathbf{W}\sim\mathcal{W}_p(n,\mathbf{C})$.

$\mathbf{W}$ szimmetriája miatt valójában $\frac{p(p+1)}{2}$-dimenziós eloszlásról van szó. *Nem centrális* Wishart-eloszlás esetén a kapcsolódó $\mathbf{X}$ mátrix oszlopvektroai $\mathcal{N}_p(\mathbf{m},\mathbf{C})$ eloszlásúak. Az $\mathbf{X}$ mátrix oszlopvektorainak segítségével $\mathbf{W}$ előállítható *diádösszegként*. *Standard Wishart-eloszlás*: $\mathcal{W}_p(n,\mathbf{I})$, a standard Wishart-eloszlás $p=1$ mellett éppen a $\chi^2(n)$-eloszlás.

Egy Wishart-mátrix standardizáltja standard Wishart-eloszlású [2, 5. fejezet, 4. szakasz, 4.1. tétel]. Azonos dimenziójú és kovarianciamátrixú Wishart-mátrixok összegének szabadságfoka az összeadandók szabadságfokainak összege [2, 5. fejezet, 4. szakasz, 4.2. állítás]. Nem elfajult p-dimenziós normális eloszlású minta mintaátlagának $\left(\bar{\mathbf{X}}\right)$, valamint empirikus kovarianciamátrix n-szeresének $(\mathbf{S})$ eloszlása [2, 5. fejezet, 4. szakasz, 4.3. tétel].

Definíciója miatt a Wishart-mátrix szimmetrikus és pozitív szemidefinit ($n>p$ esetén belátható, hogy majdnem biztosan pozitív definit is).

Paraméterbecslés

Legyen $\mathbf{X}_1,\mathbf{X}_2,\ldots,\mathbf{X}_n$ független elemű minta az $\mathbf{X}\sim\mathcal{N}_p(\mathbf{m},\mathbf{C})$ véletlen vektorra, tegyük fel, hogy $n>p$. A mintaelemek alapján szeretnénk becslést adni az ismeretlen $\mathbf{m}$ várható érték vektorra és a $\mathbf{C}$ kovarianciamátrixra, melyről feltesszük, hogy pozitív definit. Ehhez a *maximum likelihood módszert használjuk*, azaz a mintaelemek együttes sűrűségfüggvényével definiált likelihood-függvényt maximalizáljuk a két ismeretlen paraméterben.

A paraméterek ML-becslése a fenti feltevések mellett: $\hat{\mathbf{m}}=\bar{\mathbf{X}}$ és $\hat{\mathbf{C}}=\frac{1}{n}\mathbf{S}$ (lásd [2, 5. fejezet, 5. szakasz, 5.1. tétel]). Így már levezehető a (standard) Wishart-mátrix sűrűségfüggvényének képlete [2, 5. fejezet, 5. szakasz, 5.2. és 5.3. tétel]. Ebből levezethető a standard Wishart-mátrix sajátértékeinek együttes sűrűsége [2, 5. fejezet, 5. szakasz, 5.4. tétel], megemlítendő, hogy véletlen mátrixok sajátértékei fontos szerepet játszanak a kvantummechanikában (Wigner Jenő).

Hipotézisvizsgálat

Az egydimenziós esethez hasonlóan bevezethetjük a következő fogalmakat: torzítatlan, elégséges, teljes statisztika. Belátható, hogy a fenti ML-becslés esetén $\bar{\mathbf{X}}$ torzítatlan, míg $\frac{1}{n}\mathbf{S}$ torzított, de $\frac{1}{n-1}\mathbf{S}$ már torzítatlan becslés, mindkét becslés erősen konzisztens, az $\left(\bar{\mathbf{X}},\frac{1}{n}\mathbf{S}\right)$ pár elégséges statisztika, az $\left(\bar{\mathbf{X}},\frac{1}{n-1}\mathbf{S}\right)$ pár pedig hatásos becslés [2, 5. fejezet, 6. szakasz eleje].

Definíció (Hotelling-féle T^2-eloszlás)**.** Legyen $\mathbf{X}\sim\mathcal{N}_p(\mathbf{0},\mathbf{I}_p)$ és $\mathbf{W}\sim\mathcal{W}_p(n,\mathbf{I}_p)$ egymástól független véletlen vektor és véletlen mátrix. Ekkor a $T^2=n\mathbf{X}^{\mathrm{T}}\mathbf{W}^{-1}\mathbf{X}$ valószínűségi változót *Hotelling-féle T^2-eloszlásúnak* nevezzük n (szabadsági fok) és p paraméterekkel.

A T^2-eloszlás a Student-féle t-eloszlás többdimenziós általánosítása. Belátható, hogy az $\mathbf{X}\sim\sim\mathcal{N}_p(\mathbf{m},\mathbf{C})$ és $\mathbf{W}\sim\mathcal{W}_p(n,\mathbf{C})$ esetben $T^2=n(\mathbf{X}-\mathbf{m})^{\mathrm{T}}\mathbf{W}^{-1}(\mathbf{X}-\mathbf{m})$ szintén T^2-eloszlású n és p paraméterekkel [2, 5. fejezet, 6. szakasz, 6.1. állítás]. A Hotelling-féle T^2-eloszlás és a Fisher-féle F-eloszlás kapcsolatát [2, 5. fejezet, 6. szakasz, 6.2. tétel] részletezi.

A következő teszteket [2, 5. fejezet, 6. szakasz, 230–234. oldal] részletezi.

Várható érték tesztelése ismert kovarianciamátrix esetén.

Egymintás eset. Az $\mathbf{X}\sim\mathcal{N}_p(\mathbf{m},\mathbf{C})$ véletlen vektorra vegyünk egy $n>p$ elemű független mintát. Teszteljük, hogy $\mathbf{m}=\mathbf{m}_0$ teljesül-e. Ha H_0 igaz, akkor

$$U_1=\left(\bar{\mathbf{X}}-\mathbf{m}_0\right)^{\mathrm{T}}\left(\frac{1}{n}\mathbf{C}\right)^{-1}\left(\bar{\mathbf{X}}-\mathbf{m}_0\right)\sim\chi^2(p),$$

ez alapján tudunk dönteni. Ez az egymintás u-próba magasabb dimenziós megfelelője.

Kétmintás eset. Az $\mathbf{X} \sim \mathcal{N}_p(\mathbf{m}_1, \mathbf{C}_1)$, $\mathbf{Y} \sim \mathcal{N}_p(\mathbf{m}_2, \mathbf{C}_2)$ véletlen vektorokra vegyünk rendre egy-egy $n, m > p$ elemű egymástól független mintát (maguk a mintaelemek is függetlenek egymástól). Teszteljük, hogy $\mathbf{m}_1 = \mathbf{m}_2$ teljesül-e. Az előzőhöz hasonló statisztikát vizsgálunk.

Várható érték tesztelése ismeretlen kovarianciamátrix esetén.

Egymintás eset. Az előző egymintás esethez hasonló statisztikát vizsgálunk, csak itt

$$T^2 = (n-1)\left(\bar{\mathbf{X}} - \mathbf{m}_0\right)^{\mathrm{T}} \hat{\mathbf{C}}^{-1} \left(\bar{\mathbf{X}} - \mathbf{m}_0\right)$$

statisztika és a korábbi Hotelling- és Fisher-eloszlás kapcsolatát felhasználva döntünk. Ez az egymintás t-próba általánosításának tekinthető.

Kétmintás eset. Hasonlóan, csak feltesszük, hogy a két minta azonos kovarianciamátrixú. Itt is a Hotelling- és Fisher-eloszlás kapcsolatát felhasználva döntünk. Ha nem tesszük fel, hogy a kovarianciamátrixok megegyeznek, akkor is létezik próba a Welch-próbához hasonlóan.

1.9. Lineáris regresszió

A tételhez kapcsolódó anyagrészek megtalálhatóak a Bolla Marianna – Krámli András: *Statisztikai következtetések elmélete* [2, 6.3–6.5. szakaszok] című könyvben.

Véletlen változó lineáris közelítése véletlen változók lineáris kombinációjával

A többváltozós regressziós problémában az Y valószínűségi változót (függő változó) szeretnénk az $X_1, X_2, \ldots, X_p$ valószínűségi változók (független változók) függvényével közelíteni legkisebb négyzetes értelemben. A lineáris regresszió esetén a legjobb

$$Y \sim \ell(\mathbf{X}) = \mathbf{a}^{\mathrm{T}}\mathbf{X} + b$$

lineáris közelítést szeretnénk megtalálni legkisebb négyzetes értelemben, azaz minimalizálni akarjuk az

$$\mathbb{E}^2\left(Y - \left(\mathbf{a}^{\mathrm{T}}\mathbf{X} + b\right)\right)$$

kifejezést az $a_1, a_2, \ldots, a_p, b$ együtthatókban. Tehát $Y = \ell(\mathbf{X}) + \epsilon$, ahol feltehető,hogy $\mathbb{E}(\epsilon) = 0$ és ennek az ϵ-nak a négyzetét akarjuk minimalizálni.

A b együttható könnyen adódik, hiszen

$$\mathbb{E}(Y) = \mathbb{E}(\ell(\mathbf{X}) + \epsilon) = \mathbf{a}^{\mathrm{T}}\mathbb{E}(\mathbf{X}) + b,$$

tehát

$$b = \mathbb{E}(Y) - \mathbf{a}^{\mathrm{T}}\mathbb{E}(\mathbf{X})$$

Térjünk át az $Y' = Y - \mathbb{E}(Y)$ és $X_i' = X_i - \mathbb{E}(X_i)$ *centralizált* változókra, melyek várható értéke nulla, és így az

$$Y' \sim \ell\left(\mathbf{X}'\right) = \mathbf{a}^{\mathrm{T}}\mathbf{X}'$$

lineáris közelítést (*regressziós síkot*) keressük legkisebb négyzetes értelemben, azaz az

$$\mathbb{E}^2\left(Y' - \mathbf{a}^{\mathrm{T}}\mathbf{X}'\right)$$

kifejezést akarjuk minimalizálni az $a_1, a_2, \ldots, a_p$ együtthatókban. Ez a négyzetes eltérés pontosan akkor minimális, ha a hiba, azaz $\epsilon = Y' - \ell(\mathbf{X}')$ kovariancia értelemben merőleges az $X_1', X_2', \ldots, X_p'$ változók által kifeszített p-dimenziós altérre, azaz

$$\mathbb{E}\left(\epsilon X_i'\right) = 0 \qquad (i = 1, 2, \ldots, p)$$

Ez az egyenletrendszer átírható a következő alakba:

$$\sum_{j=1}^{p} \mathrm{Cov}\left(X_i, X_j\right) a_j = \mathrm{Cov}\left(X_i, Y\right) \qquad (i = 1, 2, \ldots, p),$$

ahol kihasználtuk ϵ és $Y', X_1', X_2', \ldots, X_p'$ definícióját. Legyen $\mathbf{C}$ az $\mathbf{X}$ kovariancia mátrixa, $\mathbf{d} = \\ = (d_1, d_2, \ldots, d_p)^{\mathrm{T}}$, ahol $d_i = \mathrm{Cov}\left(X_i, Y\right)$. Ekkor tömörebb alakba írhatjuk az egyenletrendszert:

$$\mathbf{Ca} = \mathbf{d},$$

a megoldás pedig a következő lesz:

$$\mathbf{a} = \mathbf{C}^{-1}\mathbf{d}.$$

Ez a közelítés maximalizálja Y és $\ell\left(\mathbf{X}\right)$ korrelációját, vagyis az X_i változók bármely másik $h\left(\mathbf{X}\right)$ lineáris kombinációja esetén Y és $h\left(\mathbf{X}\right)$ korrelációja kisebb lesz.

A lineáris modell: legkisebb négyzetek módszere

Az előző módszerhez nagyon hasonló, azonban determinisztikus változókkal dolgozunk véletlen változók helyett. Legyenek ezek a determinisztikus változók $x_1, ..., x_p$, melyek mérési pontok, előre adottak. Méréseink ezek valamilyen $a_1, ..., a_p$ paraméterekkel vett lineáris kombinációira vonatkoznak és mérési hibával terheltek. A mérési hibákat ϵ, a mérések értékét pedig Y jelöli (valószínűségi változó). Feltehető, hogy a hibák várható értéke nulla. A modell a következő tehát:

$$Y = a_1 x_1 + ... + a_p x_p + \epsilon.$$

Célunk az, hogy az ismeretlen $\mathbf{a}$ paramétervektort n mérés alapján megbecsüljük legkisebb négyzetes értelemben. Vezessük be a következő jelöléseket:

$$\mathbf{Y} = (Y_1, ..., Y_n)^{\mathrm{T}};$$
$$\epsilon = (\epsilon_1, ..., \epsilon_n)^{\mathrm{T}},$$

az i-ik méréshez tartozó p-dimenziós pontokat pedig írjuk be egy $\mathbf{X}$ mátrix soraiba. Tehát a modell $\mathbf{Y} = \mathbf{Xa} + \epsilon$ alakot ölt. Feltesszük, hogy a mérési hibák korrelálatlanok és azonos szórásúak, ekkor a mérések is korrelálatlanok és ugyanaz a kovarianciamátrixuk, mint ϵ-é: $\sigma^2\mathbf{I}_n$. Felírva a mérési hibák négyzetösszegét, majd az $\mathbf{a}$ vektor szerint deriválva jutunk a *Gauss-féle normálegyenlethez*:

$$\mathbf{X}^{\mathrm{T}}\mathbf{Xa} = \mathbf{X}^{\mathrm{T}}\mathbf{Y},$$

amit átalakítva:

$$\hat{\mathbf{a}} = \left(\mathbf{X}^{\mathrm{T}}\mathbf{X}\right)^{-1}\mathbf{X}^{\mathrm{T}}\mathbf{Y},$$

ha az $\mathbf{X}^{\mathrm{T}}\mathbf{X}$ mátrix rangja $r = p\,(\leq n)$, ha pedig szinguláris, akkor a pszeudoinverzével dolgozunk. Ez első esetben $\hat{a}$ lineáris becslés torzítatlan és minimális kovarianciamátrixú az $\mathbf{a}$-ra vonatkozó lineáris torzítatlan becslések között.

A σ^2 közös szórásnégyzet torzítatlan becslése $(r = p)$:

$$\hat{\sigma}^2 = \frac{\left(\mathbf{Y} - \mathbf{X}\hat{\mathbf{a}}\right)^{\mathrm{T}}\left(\mathbf{Y} - \mathbf{X}\hat{\mathbf{a}}\right)}{n - p}.$$

Varianciaanalízis

A varianciaanalízis speciális lineáris modelleket vizsgál, kísérlettervezésben és minőségellenőrzésben felmerülő hipotézisek tesztelésére. A tekintett modellek specifikuma az, hogy a legkisebb négyzetek módszerénél alkalmazott modellben a beállítható mérési pontok mátrixa helyett 0-1 elemekből álló ún.

struktúramátrixszal dolgozunk, amelyet úgy állítunk össze, hogy bizonyos megfigyelések csak bizonyos paraméterektől függjenek.

Gyakorlati alkalmazásokban olyan mintákat vizsgálunk, melyeket különböző körülmények közt figyeltünk meg, és célunk éppen annak a megállapítása, vajon ezek a körülmények jelentősen befolyásolják-e a mért értékeket. Tehát mintánkat eleve csoportokba osztottan kapjuk, feltesszük azonban, hogy a különböző csoportokban felvett minták egymástól függetlenek, normális eloszlásúak és azonos szórásúak.

Egyszempontos variancianalízis. Valamilyen szempont alapján (például különböző kezelések) több csoportban külön végzünk megfigyeléseket. A mintaelemek várható értékét felbonthatjuk a várhatóértékek súlyozott átlagára és a csoporthatásra. Egy lineáris modellt kapunk, a paramétereket a legkisebb négyzetek módszerével becsüljük. A mintaelemek teljes mintaátlagtól vett eltéréseinek négyzetösszege felbomlik egy csoportok közötti, illetve egy csoportokon belüli részre.

A modellben először azt a hipotézist teszteljük, hogy a várhatóértékek súlyozott átlaga nulla. Ha ezt elutasítjuk, azaz az összes várhatóérték nem nulla (van főhatás), akkor azt a hipotézist vizsgáljuk, hogy a várható értékek másik „összetevője", azaz a csoportok hatása minden esetben nulla. A hipotézis tesztelésére F-próba alkalmazható.

Kétszempontos variancianalízis (interakció nélkül). Két különböző szempont alapján végzünk kísérleteket. Például van k-féle technológia és p-féle gép, akkor kp csoportban végezzük a kísérleteket. Az egyes csoportokban tegyük fel, hogy csak egyetlen mérést végzünk és hogy a két tényező között nincs kölcsönhatás. Az összminta elemszáma így $n = kp$ és a mintaelemek függetlenek és azonos szórásúak. Egy kéttényezős lineáris modellt kapunk így. Ekkor a mintaelemek teljes mintaátlagtól vett eltéréseinek négyzetösszege három részre bontható, csoportokon belüli, illetve a csoportok közötti részre, mely a két csoport miatt két részre bontható.

Az előző esettel analóg módon, most a mintaelemek várható része 3 tényezőre bontható fel, és először megint azt a hipotézist teszteljük, hogy a várhatóértékek súlyozott átlaga nulla. Ha ezt elutasítjuk, akkor kétféle nullhipotézist kell vizsgálni, az egyik és a másik szempont szerint is megnézni, hogy a csoporthatások nullák-e. Tesztelés megint csak F-próbával, elutasítás esetén pedig t-próbával vizsgálhatóak az egyes faktorok különböző szintjei közti eltérések.

1.10. Kontingenciatáblák elemzése

Korrespondenciaanalízis

Feltesszük a továbbiakban, hogy minden eloszlás diszkrét és véges. A korrespondanciaanalízis kategórikus változók közti kapcsolatok elemzésére szolgál a változókategóriák metrikus megjelenítése alapján. Kategórikus, más néven kvalitatív változó alatt olyan diszkrét eloszlású valószínűségi változót értünk, amely véges sok értéket vesz fel, és az értékek általában nem nagyságrendet tükröznek, hanem csak a változó lehetséges értékeit kódolják (pl. a hajszín változó szőke, barna, fekete, vörös értékei az 1, 2, 3, 4 számokkal kódolhatók). A továbbiakban csak két kategórikus változót vizsgálunk, az adatok kontingenciatábla (gyakoriság- vagy relatív gyakoriságtábla) formájában vannak megadva.

A probléma a következő: az X és Y diszkrét valószínűségi változók n illetve m különböző kategóriát tartalmaznak, az egyszerűség kedvéért jelölje értékkészletüket az $\{1, 2, \ldots, n\}$ ill. az $\{1, 2, \ldots, m\}$ halmaz. X és Y nem függetlenek, értékeiket nem specifikáljuk, célunk éppen az értékek alkalmas megválasztása lesz. Egy közös megfigyelésükre vonatkozó minta alapján adva van egy $n \times m$-es *kontingenciatábla* az f_{ij} úgynevezett *cellagyakoriságokkal*, ahol f_{ij} az X változó i-edik, az Y változó j-edik kategóriájába eső megfigyelések számát jelenti.

Célunk a kontingenciatáblának valamilyen alacsonyabb rangú táblával való közelítése. Csak a 2 rangú közelítéssel foglalkozunk, ami visszavezethető a *Rényi-féle maximálkorreláció feladatára*: adott

két kategórikus változó együttes eloszlása (együttes relatív gyakorisága, azaz egy $n \times m$ gyakoriságtábla). Keressük azokat az α és β valós számértékű véletlen vektorokat, amelyek marginális eloszlásai megegyeznek az adott kontingencia táblából számolt marginális eloszlásokkal, és az együttes eloszlás alapján számított korrelációjuk maximális. Ezen véletlen vektorok együttes eloszlása az eredeti kontingenciatábla 2 rangú közelítése.

Információelméleti módszerek
A vizsgált eloszlások tipikus példája, a d-szempontos osztályozás, amikor a valószínűségek egy d-dimenziós tömbbe vannak rendezve. Az i-edik szempont kategóriáinak számát jelölje r_i. Ekkor az $(\Omega, \mathcal{A}, \mathbb{P})$ valószínűségi mező esetén az Ω elemei

$$\omega = (j_1, ..., j_d) \qquad (1 \leq j_i \leq r_i)$$

alakúak, ezeket nevezzük celláknak. Az $\mathbf{X}(\omega)$ cellagyakoriságokból álló mintát *d-dimenziós kontingenciatáblának*, pontosabban $r_1 \times \ldots \times r_d$ méretű táblának nevezzük (a jegyzetben megtalálható a $d = 2$, $r_1 = 3$, $r_2 = 3$ eset illusztrálása).

Célunk az, hogy a többdimenzós gyakoriságtáblázatok mögötti eloszlást minél kevesebb paraméterrel írjuk le *információelméleti módszerek* segítségével. A becslési feladatoknak két típusát különböztetjük meg.

Külső feltételekkel meghatározott feladatok. Ebben az esetben feltételezzük, hogy az $\mathbf{X}$ minta p valódi eloszlása egy $\mathcal{F}$ eloszláscsaládhoz tartozik. A $p \in \mathcal{F}$ eloszlás meghatározásának általánosan elfogadott módja, hogy megkeressük azt a $p^* \in \mathcal{F}$ eloszlást amely az alább ismertetett eltérések valamelyikének értelmében legközelebb van a p_X empirikus eloszláshoz. Ugyanez a módszer alkalmazható annak a hipotézisnek a vizsgálatára, hogy az $\mathbf{X}$ minta származhat-e egy $\mathcal{F}$-beli eloszlásból.

Belső feltételekkel meghatározott (modellalkotási) feladatok. Itt az $\mathbf{X}$ mintában foglalt információt kevesebb adattal, általában bizonyos $S_1, ..., S_r$ statisztikák mintabeli átlagaival kívánjuk reprezentálni. Ha ismereteink mintavétel előtti állapotát egy q eloszlás jellemzi, akkor az

$$\mathcal{F} = \left\{ p \colon \sum_{\omega \in \Omega} p(\omega) S_i(\omega) = \sum_{\omega \in \Omega} p_X(\omega) S_i(\omega) \ \ (i = 1, 2, \ldots, r) \right\}$$

eloszláshalmazhoz legközelebbi p^* eloszlást tekintjük a modellalkotási feladat megoldásának.

Eloszlások eltérése: eloszlások egymástól való eltérésére több, az információelméletben használatos mérőszám ismeretes. A kontingenciatáblák elemzésekor alapfeladat az, hogy egy eloszláscsaládnak megkeressük egy adott p eloszlástól a legkevésbé eltérő elemét. Ezt megtehetjük az *I-vetület* vagy a *L-vetület* kiszámításával.

1.11. Diszkrét idejű Markov-láncok

A tételhez kapcsolódó anyagrészek megtalálhatóak a Pap Gyula – Szűcs Gábor: *Sztochasztikus folyamatok* [11] című jegyzetben.

Sztochasztikus folyamat, példák. Lásd [11, 3–4. oldal].

Diszkrét idejű Markov-lánc, átmenetvalószínűség, Markov-tulajdonság, példák. Lásd [11, 12–16. oldal].

Homogenitás, multiplikációs formula. Lásd [11, 19–20. oldal].

Többlépéses átmenetmátrix, Chapman – Kolmogorov-egyenletek. Lásd [11, 22. oldal].

Kommunikációs osztályok, állapotok periódusa, szolidaritási tétel. Lásd [11, 24–26. oldal].

Erős Markov-tulajdonság. Lásd [11, 29–30. oldal].

Állapotok típusai, szolidaritási tétel. Lásd [11, 39–44. oldal].

Véletlen bolyongás, Pólya-tétel. Lásd [11, 45–47. oldal].

Invariáns eloszlás és mérték. Lásd [11, 48–55. oldal].

Játékos csődje probléma. Lásd [11, 62–64. oldal] (érdemes átnézni előtte a diszkrét potenciálelméletes részt).

Érdemes lehet még átnézni a következőket.

Alosztályok. Lásd [11, 28. oldal].

Visszatérési idők, visszatérés valószínűsége. Lásd [11, 32. oldal].

Ergodikus tétel. Lásd [11, 55–57. oldal].

1.12. Folytonos idejű Markov-láncok

A tételhez kapcsolódó anyagrészek megtalálhatóak a Pap Gyula – Szűcs Gábor: *Sztochasztikus folyamatok* [11] című jegyzetben.

Sztochasztikus folyamat, példák. Lásd [11, 3–4. oldal].

Felújítási folyamat, elemi felújítási tétel, Poisson-folyamat és tulajdonságai. Lásd [11, 74–77. oldal].

Folytonos Markov-lánc. Lásd [11, 83–85. oldal].

Generátormátrix, Kolmogorov egyenletei. Lásd [11, 86–90. oldal].

Állapotok típusai, kommunikációs osztályok. Lásd [11, 100–102. oldal].

Invariáns eloszlás és mérték. Lásd [11, 103–106. oldal].

Érdemes lehet még átnézni a következőket.

Càdlàg, beágyazott folyamat. Lásd [11, 93–95. oldal].

1.13. Sztochasztikus folyamatok alapfogalmai

A tételhez kapcsolódó anyagrészek megtalálhatóak a Pap Gyula – Szűcs Gábor: *Sztochasztikus folyamatok* [11] című jegyzetben.

Sztochasztikus folyamat, példák. Lásd [11, 3–4. oldal].

Kolmogorov-egzisztenciatétel. Lásd [11, 110–111. oldal].

Modifikáció. Lásd [11, 111–113. oldal].

Sztochasztikus folyamatok folytonossága. Lásd [11, 116. oldal].

Gauss-folyamatok. Lásd [11, 122–123. oldal].

Wiener-folyamatok. Lásd [11, 124–125. oldal].

Brown-híd. Lásd [11, 126. oldal].

Néhány egyéb tulajdonsága a Wiener-folyamatoknak: [1, 106–111. dia].

1.14. Optimalizálási eljárások

Alapfeladat és speciális esetei

Legyen $c\colon \mathbb{R}^n \supseteq \operatorname{dom} c \to \mathbb{R}$ a *célfüggvény*, ekkor az optimalizálás feladata a c célfüggvény minimalizálása előre kiszabott feltételek mellett:

$$\begin{array}{rcl} \mathbf{x} & \in & \mathcal{F} \\ \hline c(\mathbf{x}) & \to & \min \end{array} \quad (\mathbf{x} \in \operatorname{dom} c)\,.$$

Explicit feltételek:

$$\begin{cases} f_i(\mathbf{x}) \le 0, & i \in [k] = \{1, 2, \ldots, k\}\,; \\ g_j(\mathbf{x}) = 0, & j \in [\ell]\,, \end{cases} \quad \Rightarrow \quad \begin{cases} f(\mathbf{x}) \preceq \mathbf{0}; \\ g(\mathbf{x}) = \mathbf{0}. \end{cases}$$

A $\mathcal{D}$ *értelmezési tartomány* a c, az f_i és a g_j függvények értelmezési tartományainak metszete. A *lehetséges megoldások halmaza*: $\mathcal{L} = \mathcal{D} \cap \mathcal{F}$. Az $(\mathbf{x}^*, p^*)$ párt *optimális helynek*, illetve *optimális értéknek* nevezzük, ha

$$c(\mathbf{x}^*) = p^* = \inf_{\mathbf{x} \in \mathcal{L}} c(\mathbf{x}) \in \mathbb{R} \cup \{-\infty\} \cup \{\infty\}\,.$$

Gyakran megelégszünk ϵ-*közelítő* $(p^* + \epsilon)$, illetve -*approximáló* $((1+\epsilon)\,p^*,\ (1-\epsilon)\,p^*)$ megoldásokkal. A problémák átfogalmazhatók a feltételek ekvivalens átalakításával, *slack*-változók bevezetésével (egyenlőtlenség kiküszöbölésére), valamint a célfüggvény monoton függvénybe történő helyettesítésével.

Feltétel nélküli optimalizálás. Legkisebb négyzetek problémája: $\|\mathbf{c} - \mathbf{A}\mathbf{x}\|^2 \to \min$ (egyenes illesztése mért adatpontokra)

LP-feladatok.

$$\begin{array}{rcl} \mathbf{A}\mathbf{x} & = & \mathbf{b} \\ \mathbf{x} & \succeq & \mathbf{0} \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \min \end{array}, \qquad \begin{array}{rcl} \mathbf{A}\mathbf{x} & \preceq & \mathbf{b} \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \min \end{array}. \tag{LP}$$

SDP-feladatok.

$$\begin{array}{rcl} \sum_{i=1}^n x_i \mathbf{A}_i & \preceq & \mathbf{B} \\ \mathbf{D}\mathbf{x} & = & \mathbf{e} \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \min \end{array}; \qquad \underbrace{\begin{array}{rcll} \langle \mathbf{A}_i, \mathbf{X} \rangle & = & b_i & i \in [k] \\ \mathbf{X} & \succeq & \mathbf{0} & \\ \hline \langle \mathbf{C}, \mathbf{X} \rangle & \to & \min & \end{array}}_{\text{I. normálforma}}; \qquad \underbrace{\begin{array}{rcl} \sum_{i=1}^n x_i \mathbf{A}_i & \preceq & \mathbf{B} \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \min \end{array}}_{\text{II. normálforma}}, \tag{SDP}$$

ahol az $\mathbf{A}_i, \mathbf{B}, \mathbf{C}, \mathbf{X}$ mátrixok szimmetrikusak.

Lagrange-módszer

$$L(\mathbf{x}; \lambda, \mu) = c(\mathbf{x}) + \lambda^{\mathrm{T}} f(\mathbf{x}) + \mu^{\mathrm{T}} g(\mathbf{x})\,. \tag{Lagrange-függvény}$$

Ha $\mathbf{x} \in \mathcal{L}$ és $\lambda \succeq \mathbf{0}$, akkor $c(\mathbf{x}) \ge L(\mathbf{x}; \lambda, \mu)$. Így

$$\tilde{c}(\lambda, \mu) = \inf_{\mathbf{x} \in \mathcal{D}} L(\mathbf{x}; \lambda, \mu)\,, \qquad \begin{array}{rcl} \lambda & \succeq & \mathbf{0} \\ \hline \tilde{c}(\lambda, \mu) & \to & \max \end{array}. \tag{duális célfüggény, duális feladat}$$

Tétel (gyengedualitás-tétel)**.** *Legyen a duális feladat optimális értéke d^*. Ekkor $p^* \geq d^*$.*

Megjegyzés. Ha egyenlőség teljesül, akkor *erős dualitás*. Ha $p^* - d^* > 0$, akkor *pozitív dualitási hézag*.

Karush – Kuhn – Tucker-tétel

Tegyük fel, hogy g_i-k affin, c, f_i-k konvex és differenciálható függvények. Erős dualitás pontosan akkor teljesül, ha létezik $\hat{\mathbf{x}}$, $\left(\hat{\lambda}, \hat{\mu}\right)$, melyek teljesítik a következő feltételeket:

(KKT–1) $\hat{\mathbf{x}}$ primál lehetséges megoldás;

(KKT–2) $\left(\hat{\lambda}, \hat{\mu}\right)$ duál lehetséges megoldás;

(KKT–3) $\hat{\mathbf{x}}$, $\left(\hat{\lambda}, \hat{\mu}\right)$ komplementárisan laza tulajdonságú, azaz

- ha $f_i(\hat{\mathbf{x}}) < 0$, akkor $\hat{\lambda}_i = 0$;
- ha $\hat{\lambda}_i > 0$, akkor $f_i(\hat{\mathbf{x}}) = 0$;

(KKT–4) $\nabla c(\hat{\mathbf{x}}) + \left(\hat{\lambda}\right)^{\mathrm{T}} \nabla f(\hat{\mathbf{x}}) + (\hat{\mu})^{\mathrm{T}} \nabla g(\hat{\mathbf{x}}) = 0.$

Ha létezik ilyen $\hat{\mathbf{x}}$, $\left(\hat{\lambda}, \hat{\mu}\right)$, akkor $\hat{\mathbf{x}}$ primál, $\left(\hat{\lambda}, \hat{\mu}\right)$ duál optimumhely.

Súlyozott párosítási probléma

Feladat. Legyen a G gráf, valamint a $c\colon E \to \mathbb{R}^+$ *élsúlyozás* adott. Keressünk maximális súlyú párosítást!

A c súlyfüggvényt azonosíthatjuk egy $\mathbf{c} \in \mathbb{R}^E$ vektorral. Legyen $\mathbf{B}$ a G gráf *pont-él illeszkedési mátrixa*. Így a feladat:

$$\underbrace{\begin{array}{rcl} \mathbf{Bx} & \preceq & \mathbf{1} \\ \mathbf{0} & \preceq & \mathbf{x} \\ \mathbf{x} & \in & \mathbb{Z}^E \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \max \end{array}}_{\text{egész feltételű LP}} \quad \rightsquigarrow \quad \underbrace{\begin{array}{rcl} \mathbf{Bx} & \preceq & \mathbf{1} \\ \mathbf{0} & \preceq & \mathbf{x} \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \max \end{array}}_{\text{LP-relaxáció}} \quad \Leftrightarrow \quad \begin{array}{rcl} \mathbf{Mx} & \preceq & \begin{bmatrix}\mathbf{1}\\ \mathbf{0}\end{bmatrix} \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \max \end{array} \quad \left(\mathbf{M} = \begin{bmatrix}\mathbf{B}\\ -\mathbf{I}_E\end{bmatrix}\right).$$

Ha G *páros*, akkor $\mathbf{B}$ (és így $\mathbf{M}$ is) *totálisan unimoduláris* (bármely aldeterminánsa -1, 0 vagy 1), és ekkor a relaxált feladat ekvivalens az eredetivel.

LP és SDP kombinatorikai alkalmazásai

Folyamprobléma és duálisa. Legyen $\mathcal{H} = \left(\vec{G}, s, t, c\right)$ hálózat: s, t rendre *forrás*, *nyelő*, c *kapacitásfüggény* ($\mathbf{c}$). Legyen a *folyamfüggvény* $f\colon E \to \mathbb{R}$, azonosíthatjuk $\mathbf{x}$-szel. Teljesüljenek a kapacitásfeltételek: $\mathbf{0} \preceq \mathbf{x} \preceq \mathbf{c}$, valamint a Kirchhoff-törvény (csúcsonként a ki- és a beáramló mennyiség azonos). A folyam *értéke*: v, a forrásnál a kiáramló és beáramló mennyiség különbsége (nyelőnél fordítva).

Adjunk hozzá $\vec{G}$-hez egy $e_+ = \overrightarrow{ts}$ élt, melyen a (kiterjesztett) folyam v-t vesz fel. Ekkor $\vec{G}_+$ cirkuláció. A feladat és duálisa:

$$\begin{array}{rcl} \mathbf{0} & \preceq \mathbf{x} \preceq & \mathbf{c} \\ \mathbf{B}_+\mathbf{x}_+ & = & \mathbf{0} \\ \hline v & \to & \max \end{array} \quad \rightsquigarrow \quad \begin{array}{rcl} \mathcal{V} & & \text{egy } s\text{-}t\text{-vágás} \\ \hline C(\mathcal{V}) & \to & \min \end{array}. \qquad \text{(MFMC)}$$

Maximális vágás problémája és duálisa. Legyen $G = (V, E)$ egyszerű gráf. Keressünk olyan $\mathcal{V}$ vágást, melyre $|E(\mathcal{V})|$ maximális! A feladat duálisa SDP-feladat ($\mathbf{A}$ a szomszédsági mátrix, $\mathbf{x} \in \{-1, 1\}^V$ a vágást kódolja):

$$\begin{array}{rcl} \mathbf{A} + \operatorname{diag}\mu & \succeq & \mathbf{0} \\ \hline -\mathbf{1}^{\mathrm{T}}\mu & \to & \max \end{array}.$$

Maximális független ponthalmaz felső becslése. Legyen $G = (V, E)$ egyszerű gráf, legyen $\mathbf{A}$ a gráf szomszédsági mátrixa. Jelölje $\mathbf{J}$ a csupa 1 mátrixot, legyen $\bar{\mathbf{A}} = \mathbf{J} - \mathbf{A}$. Ekkor, ha $F \subseteq V$ független ponthalmaz, akkor $\bar{\mathbf{A}}\big|_{F\times F} = \mathbf{J}$. Sajátvektor-sajátértékekre vonatkozó észrevételekből adódik, hogy $|F| \leq \lambda_{\max}\left(\bar{\mathbf{A}}\right)$, és így $\alpha(G) \leq \lambda_{\max}\left(\bar{\mathbf{A}}\right)$.

A kapcsolódó SDP-feladat:

$$\begin{array}{rcl} \mathbf{M} & = & \mathbf{J} - \sum_{e\in E} x_e \mathbf{S}_e \\ \mu\mathbf{I}_V - \mathbf{M} & \succeq & \mathbf{0} \\ \hline \mu & \to & \min. \end{array}$$

Ennek a feladatnak a optimumát a *G gráf Lovász-féle θ-függvényének* nevezzük, és $\alpha(G) \leq \leq \theta(G)$.

Lovász-féle szendvicstétel: $\alpha(G) \leq \theta(G) \leq \bar{\chi}(G)\left(= \chi\left(\bar{G}\right)\right)$.

Egészértékű programozás

$$\begin{array}{rcl} \mathbf{A}\mathbf{x} & \preceq & \mathbf{b} \\ \mathbf{x} & \in & \mathbb{N}^n \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \min. \end{array} \qquad \rightsquigarrow \qquad \begin{array}{rcl} \mathbf{A}\mathbf{x} & \preceq & \mathbf{b} \\ \hline \mathbf{c}^{\mathrm{T}}\mathbf{x} & \to & \min. \end{array} \qquad \text{(IP és LP-relaxáltja)}$$

L-következtetés. Szokásos „levezetés” révén nyert új egyenlőtlenség.

I-következtetés. Ha $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \leq \beta$ az egyenlőtlenségek egy következménye (L-következtetés), akkor $\lfloor\alpha_1\rfloor x_1 + \lfloor\alpha_2\rfloor x_2 + \ldots + \lfloor\alpha_n\rfloor x_n \leq \lfloor\beta\rfloor$ egy *I-köveztetés*. Az új egyenlőtlenségnek a feltételekhez történő hozzáadásával nem veszítünk lehetséges megoldást.

Algoritmus. L- és I-következtetések végrehajtását (valamilyen sámát követve, pl. Gomory-algoritmust) követően megoldjuk a kapcsolódó LP-relaxált feladatot, ha a kapott megoldás egész koordinátájú, akkor készen vagyunk, ha nem, akkor új L- és I-következtetéseket hajtunk végre, és így tovább...

Korlátozás és szétválasztás módszerek alkalmazásai

Feltétel nélküli optimalizálás. $c(\mathbf{x})$-et szeretnénk minimalizálni (létezik optimum, elég egy ϵ-közelítő megoldás). Legyen adott egy T_0 tégla, aminek eleme az optimumhely. Tegyük fel, hogy c „szép”: minden téglán könnyen adhatunk alsó és felső becslést c-re; egy tégla (egy oldala menti) kettévágásával ezek a becslések javulnak; ha a téglalap egy ponthoz közelít, akkor az alsó és felső becslések különbsége kicsi (ϵ) lesz.

Az algoritmus dióhéjban: Téglalapfelezgetéssel közelítünk egy ϵ-közelítő megoldáshoz; egy téglát a leghosszabb oldala mentén felezünk; azon tégla „irányába” indulunk, amelyikre a legkisebb az alsó becslés (csak a „leveleket” tartjuk számon).

Vegyes konvex-egész optimalizálás. Legyen $\mathbf{d} \in \{0, 1\}^m$, c, f_i ($i \in [k]$) konvex függvények. A feladat:

$$\begin{array}{rcl} f(\mathbf{x}, \mathbf{d}) & \preceq & 0 \\ \hline c(\mathbf{x}, \mathbf{d}) & \to & \min \end{array}.$$

Kevés nemnulla komponens lineáris feltételek mellett. Egy egyenlőtlenségrendszer olyan megoldását keressük, melynek kevés nemnulla komponense van. Ez visszavezethető egy vegyes konvex-egész optimalizálási feladatra.

2. Általános szakirány tételei

2.1. Mátrixok sajátértékeinek meghatározása

A tételhez kapcsolódó anyagrészek megtalálhatóak Móricz Ferenc: *Bevezetés a numerikus matematikába* [9] és Móricz Ferenc: *Numerikus módszerek az algebrában és analízisben* [8] című könyveiben.

Mátrixok trianguláris felbontása, ortogonális triangularizáció

Lásd [8, I. fejezet, 1. szakasz].

Egy $\mathbf{A}$ négyzetes mátrix *trianguláris felbontása* ($\mathbf{A} = \mathbf{LU}$) nem minden esetben létezik, még akkor sem, ha a mátrix nemszinguláris. Viszont ha a balfelső főminorok mind 0-tól különbözőek, akkor a felbontás létezik és a felső trianguláris $\mathbf{U}$ mátrix diagonális elemei a balfelső főminorok segítségével meghatározhatóak és ekkor $\mathbf{U}$ sem szinguláris. Ha az $\mathbf{A}$ mátrix valamely balfelső főminora abszolútértékben kicsi, akkor a trianguláris felbontás során fellépő osztások során olyan kerekítési hibák léphetnek fel, amelyek az eljárás végehajthatóságát veszélyeztethetik a túl kicsi/nagy számokkal történő számolások következtében, vagy pedig teljesen eltorzíthatják az $\mathbf{L}$ és $\mathbf{U}$ mátrixok elemeit. Ez a probléma kiküszöbölhető egy másik típusú, ún. *ortogonális triangularizáció* segítségével, ahol az alulról trianguláris $\mathbf{L}$ mátrixot egy ortogonális $\mathbf{Q}$ mátrixszal helyettesítjük és egy felülről trianguláris $\mathbf{U}$ mátrixot továbbra is megtartunk.

Ha az $\mathbf{A}$ mátrix nemszinguláris, akkor az $\mathbf{LU}$ felbontás egyértelmű, míg a $\mathbf{QU}$ felbontás a $\mathbf{Q}$ oszlopainak és $\mathbf{U}$ sorainak előjelétől eltekintve egyértelmű.

Tetszőleges téglalap alakú mátrix ortogonális triangularizációja is definiálható a 3. tétel segítségével.

LR-algoritmus

Lásd [8, I. fejezet, 3. szakasz].

Legyen $\mathbf{A}$ négyzetes mátrix, melynek sajátértékeit meg szeretnénk határozni. Az LR-algoritmus segítségével a következő módon határozhatjuk meg a sajátértékeket:

1: $\mathbf{A}_1 \leftarrow \mathbf{A}$
2: $(\mathbf{L}_1, \mathbf{R}_1) \leftarrow$ TriangulárisFelbontás$(\mathbf{A}_1)$
3: **for** $s \leftarrow 1, s \leftarrow s + 1$ **do**
4: $\quad \mathbf{A}_{s+1} \leftarrow \mathbf{R}_s \mathbf{L}_s$
5: $\quad (\mathbf{L}_{s+1}, \mathbf{R}_{s+1}) \leftarrow$ TriangulárisFelbontás$(\mathbf{A}_{s+1})$

Legyen $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$ az $\mathbf{A}$ sajátvektoraiból alkotott mátrix és $\Lambda = \operatorname{diag}[\lambda_1, \lambda_2, \ldots, \lambda_n]^{\mathrm{T}}$ az $\mathbf{A}$ sajátértékeiből képzett diagonális mátrix (feltéve, hogy $|\lambda_1| > |\lambda_2| > \ldots > |\lambda_n| > 0$). Ha $\mathbf{X}$ és $\mathbf{X}^{-1}$ balfelső főminorai 0-tól különbözőek, akkor az $\{\mathbf{A}_s \colon s = 1, 2, 3, \ldots\}$ mátrixsorozat konvergens, határértéke egy olyan felülről trianguláris mátrix, melynek főátlójában a $\lambda_1, \lambda_2, \ldots, \lambda_n$ sajátértékek állnak.

Az előző algoritmus bármely lépésben elakadhat, ha nem létezik a trianguláris felbontás. Ha a trianguláris felbontás során *részleges főelemkiválasztást* alkalmazunk, akkor a *módosított LR-algoritmus* nem akadhat el, ha a szóban forgó mátrix nemszinguláris.

QR-algoritmus

Lásd [8, I. fejezet, 4. szakasz].

Teljesen hasonló az LR-algoritmushoz, csak a trianguláris felbontás helyett ortogonális triangularizációra van szükség.

R^HR-algoritmus

Lásd [9, II. fejezet, 5. szakasz].

`Ezt még nem néztem meg a másik Móricz-könyvben - JR.`

2.2. Mátrixok általánosított inverze

A tételhez kapcsolódó anyagrészek megtalálhatóak Móricz Ferenc: *Numerikus módszerek az algebrában és analízisben* [8, II. fejezet] című könyveiben.

Motiváció

Az *általánosított inverz* bevezetésével definiálni tudunk egy olyan mátrixot szinguláris négyzetes mátrixok és nem négyzetes mátrixok esetén is, amely hasonló tulajdonságokkal rendelkezik, mint a hagyományos inverzmátrix, illetve négyzetes nemszinguláris mátrixok esetén megegyezik a hagyományos inverzmátrixszal.

Kiszámítás rangfaktorizációval

Lásd [8, II. fejezet, 6. szakasz].

Egy tetszőleges mátrix előállítható egy *oszlopreguláris* és egy *sorreguláris* mátrix szorzataként (rangfaktorizáció). A sor-/oszlopreguláris mátrixok általánosított inverze számolható az 1. és 2. definíciók szerint. Az általános definíciót ezen definíciók és a rangfaktorizáció segítségével kapjuk.

Kiszámítás particionálással

Lásd [8, II. fejezet, 8. szakasz].

Inverzmátrix Frobenius módszerével történő kiszámításának általánosítása. *Rang szerint particionált mátrix* általánosított inverze „könnyen” számítható a 29. tétel segítségével. Tetszőleges mátrix két *szimmetrikus permutáló mátrix* segítségével rang szerint particionált alakra hozható, mely mátrixnak ki tudjuk számolni az általánosított inverzét. A 30. tételben megtalálható, hogy ezek alapján hogyan jön ki egy tetszőleges mátrix általánosított inverze particionálással.

Kiszámítás ortogonális triangularizációval

Lásd [8, II. fejezet, 8. szakasz utolsó megjegyzése].

Lineáris egyenletrendszerek vizsgálata

Lásd [8, II. fejezet, 7. szakasz].

Bizonyos *kompatibilitási feltételek* esetén a kapcsolódó lineáris egyenletrendszereknek megadhatók az általános megoldásai (22. és 23. tétel), illetve az egyetlen normál megoldás (26. és 27. tétel).

2.3. Periodikus függvények diszkrét négyzetes közelítése

A tételhez kapcsolódó anyagrészek megtalálhatóak a Móricz Ferenc: *Numerikus módszerek az algebrában és analízisben* [8, V. fejezet, 21. és 22. szakaszok] című könyvben.

DFT – diszkrét Fourier-transzformáció, IDFT – inverz diszkrét Fourier-transzformáció

Lásd [8, V. fejezet, 21. szakasz].

Olyan függvényeket szeretnénk közelíteni, melyeknek értékét bizonyos diszkrét pontsorozatokon ismerjük (általában mérési adatokból, de a hiba igen nagy is lehet). Ilyen függvények közelítésére az interpoláció már nem megfelelő, a legkisebb négyzetek elve alapján számított, ún. *legjobb négyzetes közelítés* általában jobb közelítést eredményez. A 2π szerint periodikus függvényeket tekintjük, alappontoknak a $[0, 2\pi)$ intervallum ekvidisztáns beosztását vesszük, alapfüggvényeknek pedig a komplex trigonometrikus függényeket választjuk. A 21. szakaszban megtaláljuk a DFT, majd rögtön utána az IDFT definícióját (121. oldal), melyek az előtte lévő levezetések alapján nyernek értelmet.

FFT - gyors Fourier-transzformáció

Lásd [8, V. fejezet, 22. szakasz első fele].

A DFT és IDFT műveletigénye n^2, ha ismerjük az n-edik komplex egységgyököket. Ha $n = 2^r$ alakú, azaz kettőnek egész kitevőjű hatványa, akkor a műveletigényben jelentős megtakarítás érhető el, mind a DFT és IDFT szervezhető olyan módon, hogy a műveletigény $n \log_2 n$ komplex szorzás legyen. A lényeg az a_q együtthatók képletében a 2^r összeadandóból kitudunk választani olyan csoportokat, amelyek különböző együtthatók kifejezésében egyaránt fellépnek. Ehhez a képletekben szereplő j és q számok diadikus előállítása szükséges.

Számsorozatok konvolúciója

Lásd [8, V. fejezet, 22. szakasz második fele].

Két vektor konvolúciója a definíció alapján $n\,(n+1)$ szorzás segítségével állítható elő. A 66. tétel (63)-as képletét átírva azonban kapjuk, hogy vektorok konvolúciója FFT segítségével is számolható, ha n kettő egész kitevőjű hatványa (n itt a vektorok hossza). Ezzel a módszerrel a számítás műveletigénye csupán $6n \log_2 n + 8n$.

2.4. A hullámegyenlet

Húr és membránok rezgései

Legyen $\Omega \subset \mathbb{R}^d$ nyílt, $u\colon \overline{\Omega} \times [0,\infty) \to \mathbb{R}$,

$$u_{tt} = \Delta_{\mathbf{x}} u; \qquad \text{(homogén)}$$
$$u_{tt} = \Delta_{\mathbf{x}} u + f, \qquad \text{(inhomogén)}$$

ahol $f = f(\mathbf{x}, t)$ adott. Az $u(\mathbf{x}, t)$ függvény az $u \equiv 0$ egyensúlyi helyzettől való eltérést méri az $\mathbf{x}$ helyen a t időben. Egydimenzióban ($d = 1$) *rezgő húr*, kétdimenzióban ($d = 2$) *membrán*, háromdimenzióban ($d = 3$) *rugalmas test*.

Megjegyzés. A továbbiakban $\Delta_{\mathbf{x}}$ helyett egyszerűen csak Δ-t írunk.

D'Alambert-formula

Legyen $u\colon \mathbb{R} \times [0,\infty) \to \mathbb{R}$,

$$\begin{aligned} u_{tt}(x,t) &= u_{xx}(x,t) \quad (x \in \mathbb{R}, t > 0); \\ u(x,0) &= g(x) \qquad\qquad (x \in \mathbb{R}); \\ u_t(x,0) &= h(x) \qquad\qquad (x \in \mathbb{R}), \end{aligned}$$

ahol $g, h\colon \mathbb{R} \to \mathbb{R}$ adott függvények $\left(g \in C^2(\mathbb{R}), h \in C^1(\mathbb{R})\right)$. Megoldás:

$$u(x,t) = \frac{1}{2}\left(g(x+t) + g(x-t)\right) + \frac{1}{2}\int_{x-t}^{x+t} h(y)\,\mathrm{d}y, \qquad \text{(D'Alambert)}$$

ahol $u \in C^2(\mathbb{R} \times [0,\infty))$, és minden $x_0 \in \mathbb{R}$ esetén

$$\lim_{\substack{(x,t)\to(x_0,0)\\ t>0}} u(x,t) = g(x_0);$$
$$\lim_{\substack{(x,t)\to(x_0,0)\\ t>0}} u_t(x,t) = h(x_0).$$

Megjegyzés. A megoldás alakja: $u(x,t) = F(x+t) + G(x-t)$.

Hullámterjedés páros és páratlan dimenzióban

Tekintsük a következőt:

$$\begin{aligned} u_{tt} - \Delta u &= 0 && \left(\mathbf{x} \in \mathbb{R}^d, t > 0\right); \\ u(\mathbf{x}, 0) &= g(\mathbf{x}) && \left(\mathbf{x} \in \mathbb{R}^d\right); \\ u_t(\mathbf{x}, 0) &= h(\mathbf{x}) && \left(\mathbf{x} \in \mathbb{R}^d\right). \end{aligned}$$

Páratlan dimenzió. Legyen $d = 2k+1$, $k \in \mathbb{N}^+$, tegyük fel, hogy $g \in C^{k+2}\left(\mathbb{R}^d\right)$, $h \in C^{k+1}\left(\mathbb{R}^d\right)$. Ekkor van megoldás, és u kiterjeszthető $\mathbb{R}^d \times [0,\infty)$-re úgy, hogy $u \in C^2\left(\mathbb{R}^d \times [0,\infty)\right)$, valamint a d'Alambert-formulához hasonló konvergencia teljesül.

- A $d = 1$ esetben, a D'ALAMBERT-formulában nem szerepel g deriváltja, míg a $d = 3, 5, 7, \ldots$ esetekben g deriváltja előfordul a formulában, így u kevésbé „szép", mint g.
- A kezdeti hatások véges (pontosan 1) sebességgel terjednek.

Páros dimenzió. Legyen $d = 2k$, $k \in \mathbb{N}^+$, tegyük fel, hogy $g \in C^{k+2}\left(\mathbb{R}^d\right)$, $h \in C^{k+1}\left(\mathbb{R}^d\right)$. Ekkor van megoldás, és u kiterjeszthető $\mathbb{R}^d \times [0,\infty)$-re úgy, hogy $u \in C^2\left(\mathbb{R}^d \times [0,\infty)\right)$, valamint a d'Alambert-formulához hasonló konvergencia teljesül.

- Adott $\mathbf{x} \in \mathbb{R}^d$-re $g(\mathbf{x})$ és $h(\mathbf{x})$ hatása, ha $d \geq 3$, páratlan, akkor azon $(\mathbf{y}, t)$ pontokban van jelen, ahol $|\mathbf{x} - \mathbf{y}| = t$; míg ha $d \geq 2$, páros, akkor azon $(\mathbf{y}, t)$ pontokban van jelen, ahol $|\mathbf{x} - \mathbf{y}| < t$.

A *Huygens-elv*: az $\mathbf{x} \in \mathbb{R}^d$ pontból kiinduló zavar

- éles hullámfront mentén terjed $d \geq 3$ páratlan dimenzióban;
- a hullámfront után is hat $d \geq 2$ páros dimenzióban.

Háromdimenzióban ($d = 3$) a megoldás a *Kirchoff-formula* (D'ALAMBERT-formulából szférikus közepekkel és Euler – Poisson – Darboux-egyenlettel). Magasabb (páratlan) dimenzióban analóg módon.

A leereszkedés módszere

Kétdimenzióban ($d = 2$) a *Poisson-formula* (Kirchoff-formulából konstans kiterjesztéssel, $\bar{u}(x_1, x_2, x_3, t) = \bar{u}(x_1, x_2, 0, t) = u(x_1, x_2, t)$). Magasabb (páros) dimenzióban analóg módon.

Duhamel-elv

Tekintsük a következőt:

$$\begin{aligned} u_{tt} - \Delta u &= f && \left(\mathbf{x} \in \mathbb{R}^d, t > 0\right); \\ u(\mathbf{x}, 0) &= 0 && \left(\mathbf{x} \in \mathbb{R}^d\right); \\ u_t(\mathbf{x}, 0) &= 0 && \left(\mathbf{x} \in \mathbb{R}^d\right). \end{aligned}$$

Legyen $s \geq 0$ esetén $u(\mathbf{x}, t; s)$ az

$$\begin{aligned} u_{tt}(\mathbf{x}, t; s) - \Delta u(\mathbf{x}, t; s) &= 0 && \left(\mathbf{x} \in \mathbb{R}^d, t > s\right); \\ u(\mathbf{x}, s; s) &= 0 && \left(\mathbf{x} \in \mathbb{R}^d\right); \\ u_t(\mathbf{x}, s; s) &= f(\mathbf{x}, s) && \left(\mathbf{x} \in \mathbb{R}^d\right). \end{aligned}$$

megoldása (ilyen van az előző formulák szerint). Ekkor

$$u(\mathbf{x}, t) = \int_0^t u(\mathbf{x}, t; s)\, \mathrm{d}s \quad \left(\mathbf{x} \in \mathbb{R}^d, t > 0\right)$$

megoldása az eredeti inhomogén problémának. Ehhez elég, hogy $f \in C^{\left[\frac{d}{2}\right]+1}\left(\mathbb{R}^d \times [0,\infty)\right)$.

2.5. A hővezetés egyenlete

Legyen $\Omega \subset \mathbb{R}^d$ nyílt, $0 < T \leq \infty$, és legyen

$$\Omega_T = \Omega \times (0,T)\,;$$
$$\partial^* \Omega_T = \left(\overline{\Omega} \times \{0\}\right) \cup (\partial\Omega \times [0,T])$$

ahol $\partial^*\Omega_T$-t nevezzük Ω_T *parabolikus határának*. Adott $f \in C^0\left(\partial^*\Omega_T\right)$. Az

$$u_t(\mathbf{x},t) = \Delta_{\mathbf{x}} u(\mathbf{x},t) \qquad ((\mathbf{x},t) \in \Omega_T)\,;$$
$$u(\mathbf{x},t) = f(\mathbf{x},t) \qquad ((\mathbf{x},t) \in \partial^*\Omega_T)$$

peremérték-probléma megoldása olyan $u\colon \overline{\Omega_T} \to \mathbb{R}$ függvény, amelyre $u \in C^0\left(\overline{\Omega_T}\right)$,

$$u(\cdot,t) \in C^2(\Omega) \qquad (\forall\, t \in (0,T))\,;$$
$$u(\mathbf{x},\cdot) \in C^1(0,T) \qquad (\forall\, \mathbf{x} \in \Omega)\,,$$

és teljesülnek u-ra a fenti egyenletek.

Cauchy-probléma megoldása
Legyen $g\colon \mathbb{R}^d \to \mathbb{R}$ adott. Olyan $u\colon \mathbb{R}^d \times [0,\infty) \to \mathbb{R}$ függvényt keresünk, amelyre

$$u_t - \Delta u = 0 \qquad \left(\forall\ (\mathbf{x},t) \in \mathbb{R}^d \times (0,\infty)\right)\,;$$
$$u(\mathbf{x},0) = g(\mathbf{x}) \qquad \left(\forall\, \mathbf{x} \in \mathbb{R}^d\right).$$

Legyen

$$\Phi(\mathbf{x},t) = \frac{1}{(4\pi t)^{\frac{d}{2}}} \mathrm{e}^{-\frac{|\mathbf{x}|^2}{4t}}. \qquad \text{(fundamentális megoldás)}$$

Ekkor $\Phi_t - \Delta_{\mathbf{x}}\Phi = 0$ egész $\mathbb{R}^d \times (0,\infty)$-en. Legyen $\mathbf{x} \in \mathbb{R}^d$ és $t > 0$ esetén

$$u(\mathbf{x},t) = \int_{\mathbb{R}^d} \Phi(\mathbf{x}-\mathbf{y},t)\, g(\mathbf{y})\, \mathrm{d}\mathbf{y}. \qquad \text{(Poisson-integrál)}$$

Tétel. *Legyen $g \in C^0\left(\mathbb{R}^d\right)$ korlátos, és definiáljuk az $u\colon \mathbb{R}^d \times [0,\infty) \to \mathbb{R}$ függvényt a fenti módon. Ekkor*

1. $u \in C^\infty\left(\mathbb{R}^d \times [0,\infty)\right)$;
2. $u_t(\mathbf{x},t) - \Delta u(\mathbf{x},t) = 0 \ \left(\mathbf{x} \in \mathbb{R}^d, t > 0\right)$;
3. *bármely $\mathbf{x}_0 \in \mathbb{R}^d$-re*
$$\lim_{\substack{(\mathbf{x},t)\to(\mathbf{x}_0,0)\\ \mathbf{x}\in\mathbb{R}^d, t>0}} u(\mathbf{x},t) = g(\mathbf{x}_0)\,.$$

Megjegyzés.

– Ha $g = \delta(0)$ (amit nem enged meg az előző tétel, hiszen $\delta(0)$ nem folytonos, korlátos), akkor

$$\Phi_t - \Delta\Phi = 0 \qquad \left(\forall\ (\mathbf{x},t) \in \mathbb{R}^d \times (0,\infty)\right)\,;$$
$$\Phi(\mathbf{x},0) = \delta(0) \qquad \left(\forall\, \mathbf{x} \in \mathbb{R}^d\right).$$

– Ha $g \geq 0$ és $g \not\equiv 0$, akkor bármely $\mathbf{x} \in \mathbb{R}^d$ és bármely $t > 0$ esetén a kezdeti g hatása ∞ sebességgel terjed.

Maximumelvek

Tétel (erős maximumelv)**.** *Tegyük fel, hogy* $u \in C^{2,1}(\Omega_T) \cap C^0\left(\overline{\Omega_T}\right)$ *és* $u_t = \Delta u$ Ω_T*-n. Ekkor*

1.

$$\max_{\overline{\Omega_T}} u = \max_{\partial^* \Omega_T} u;$$

2. ha Ω *összefüggő és létezik* $(\mathbf{x}_0, t_0) \in \Omega_T$ *úgy, hogy* $u(\mathbf{x}_0, t_0) = \max_{\overline{\Omega_T}} u$ *akkor* u *állandó* $\overline{\Omega_{t_0}}$*-on.*

Megjegyzés.

– Csak $\overline{\Omega_{t_0}}$-on állítjuk, hogy u állandó, mivel $t > t_0$-ra nem feltétlenül igaz.

– Ha u megoldása az

$$\begin{aligned} u_t &= \Delta u && \Omega_T\text{-n;} \\ u &= 0 && \partial\Omega \times [0,T]\text{ -n;} \\ u &= g && \Omega \times \{0\}\text{ -n} \end{aligned}$$

problémának, továbbá $g(\mathbf{x}) \geq 0$ Ω-n és $g \not\equiv 0$, akkor $u(\mathbf{x}, t) > 0$ Ω_T-n.

Tétel (egyértelműség)**.** *Tegyük fel, hogy* $g \in C^0(\partial^* \Omega_T)$*,* $f \in C^0(\Omega_T)$*. Ekkor az*

$$\begin{aligned} u_t - \Delta u &= f && \Omega_T\text{-}n\text{;} \\ u &= g && \partial^* \Omega_T\text{-}n \end{aligned}$$

problémának legfeljebb egy $u \in C^{2,1}(\Omega_T) \cap C^0\left(\overline{\Omega_T}\right)$ *megoldása van.*

Tétel (maximumelv $\mathbb{R}^d$-ben)**.** *Tegyük fel, hogy* $u \in C^{2,1}\left(\mathbb{R}^d \times (0,T]\right) \cap C^0\left(\mathbb{R}^d \times [0,T]\right)$ *az*

$$\begin{aligned} u_t &= \Delta u && \mathbb{R}^d \times (0,T)\text{ -}n\text{;} \\ u &= g && \mathbb{R}^d \times \{0\}\text{ -}n \end{aligned}$$

probléma megoldása, továbbá

$$u(\mathbf{x}, t) \leq A \mathrm{e}^{a|\mathbf{x}|^2} \quad \left(\mathbf{x} \in \mathbb{R}^d, 0 \leq t \leq T\right)$$

valamely $A, a > 0$ *esetén. Ekkor*

$$\sup_{\mathbb{R}^d \times [0,T]} u = \sup_{\mathbb{R}^d} g.$$

Tétel (egyértelműség $\mathbb{R}^d$-ben)**.** *Legyen* $T > 0$*,* $g \in C^0\left(\mathbb{R}^d\right)$*,* $f \in C^0\left(\mathbb{R}^d \times [0,T]\right)$*. Ekkor legfeljebb egy olyan* $u \in C^{2,1}\left(\mathbb{R}^d \times (0,T)\right) \cap C^0\left(\mathbb{R}^d \times [0,T]\right)$ *megoldása van az*

$$\begin{aligned} u_t &= \Delta u && \mathbb{R}^d \times (0,T)\text{ -}n\text{;} \\ u &= g && \mathbb{R}^d \times \{0\}\text{ -}n \end{aligned}$$

problémának, amelyre teljesül

$$|u(\mathbf{x}, t)| \leq A \mathrm{e}^{a|\mathbf{x}|^2} \quad \left(\mathbf{x} \in \mathbb{R}^d, 0 \leq t \leq T\right)$$

valamely $A, a > 0$ *állandókkal.*

Megjegyzés. Az

$$\begin{aligned} u_t &= \Delta u && \mathbb{R}^d \times (0,T)\text{-n;} \\ u &= 0 && \mathbb{R}^d \times \{0\}\text{-n} \end{aligned}$$

problémának az $u \equiv 0$ megoldás mellett lehet olyan megoldása, amelyre nem teljesül a fenti korlát.

Az

$$\begin{aligned} u_t &= \Delta u; \\ u(\mathbf{x},0) &= f(\mathbf{x}) \end{aligned}$$

problémának általában nincs visszafelé (azaz $t < 0$-ra) megoldása. De ha van, akkor az egyértelmű.

2.6. A Laplace-egyenlet

Harmonikus függvény

Legyen $\Omega \subset \mathbb{R}^d$ korlátos, nyílt, $\partial\Omega$ C^1-sima.

Definíció (harmonikus függvény)**.** Az $u \in C^2(\Omega)$ függvény *harmonikus*, ha $\Delta u = 0$ Ω-n.

Példa. $\mathbb{R}^d$-ben

- $u(\mathbf{x}) = \mathbf{a}^{\mathrm{T}}\mathbf{x} + b$;
- $u(\mathbf{x}) = x_1^2 - x_2^2$ $(d \geq 2)$;
- $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$, $\mathbf{x} \neq \mathbf{y}$:

$$\Gamma(\mathbf{x},\mathbf{y}) = \Gamma(|\mathbf{x}-\mathbf{y}|) = \begin{cases} \frac{1}{2\pi}\log|\mathbf{x}-\mathbf{y}|, & \text{ha } d=2; \\ \frac{1}{d(2-d)\omega_d} \cdot \frac{1}{|\mathbf{x}-\mathbf{y}|^{d-2}}, & \text{ha } d \geq 3. \end{cases}$$

Megjegyzés. A fenti Γ a $\Delta u = 0$ Laplace-egyenlet *fundamentális megoldása* és harmonikus $\mathbb{R}^d \setminus \{\mathbf{y}\}$-on.

Green-függvény

Definíció (Green-függvény)**.** A $G(\mathbf{x},\mathbf{y})$ függvény $(\mathbf{x},\mathbf{y} \in \Omega, \mathbf{x} \neq \mathbf{y})$ *Green-függvény*, ha

1. $G(\mathbf{x},\mathbf{y}) = 0$ bármely $\mathbf{x} \in \partial\Omega$-ra;
2. $\mathbf{x} \mapsto G(\mathbf{x},\mathbf{y}) - \Gamma(\mathbf{x},\mathbf{y})$ harmonikus Ω-n.

Megjegyzés. Ha u harmonikus Ω-n, akkor

$$u(\mathbf{y}) = \int_{\partial\Omega} u(\mathbf{x}) \frac{\partial G}{\partial \nu_{\mathbf{x}}}(\mathbf{x},\mathbf{y}) \, \mathrm{d}\sigma,$$

azaz u-t meghatározza $u|_{\partial\Omega}$ (a Green-féle reprezentációs formulából következik).

Green-függvény konstrukciója gyakran „tükrözéssel” $\partial\Omega$-ra, $G(\mathbf{x},\mathbf{y}) = \Gamma(\mathbf{x},\mathbf{y}) - \Gamma(\mathbf{x},\tilde{\mathbf{y}})$.

Példa. Legyen

$$\tilde{\mathbf{y}} = \begin{cases} \frac{R^2}{|\mathbf{y}|^2}\mathbf{y}, & \text{ha } \mathbf{y} \neq \mathbf{0}; \\ \infty, & \text{ha } \mathbf{y} = \mathbf{0}, \end{cases}$$

valamint legyen

$$G(\mathbf{x},\mathbf{y}) = \begin{cases} \Gamma(|\mathbf{x}-\mathbf{y}|) - \Gamma\left(\frac{|\mathbf{y}|}{R}|\mathbf{x}-\tilde{\mathbf{y}}|\right), & \text{ha } \mathbf{y} \neq \mathbf{0}; \\ \Gamma(|\mathbf{x}|) - \Gamma(R), & \text{ha } \mathbf{y} = \mathbf{0}. \end{cases}$$

Ekkor G Green-függvénye $\mathbb{B}(\mathbf{0},R)$-nek, és

$$u(\mathbf{y}) = \frac{R^2-|\mathbf{y}|^2}{d\omega_d R}\int_{\partial\mathbb{B}(\mathbf{0},R)} \frac{u(\mathbf{x})}{|\mathbf{x}-\mathbf{y}|^d}\,\mathrm{d}\sigma.$$

Poisson-formula

Tétel (Poisson-formula gömbre)**.** *Legyen $\phi\colon \partial\mathbb{B}(\mathbf{0},R) \to \mathbb{R}$ folytonos, adott. Ekkor az*

$$u(\mathbf{y}) = \begin{cases} \frac{R^2-|\mathbf{y}|^2}{d\omega_d R}\int_{\partial\mathbb{B}(\mathbf{0},R)} \frac{\phi(\mathbf{x})}{|\mathbf{x}-\mathbf{y}|^d}\,\mathrm{d}\sigma, & \textit{ha } \mathbf{y} \in \operatorname{int}\mathbb{B}(\mathbf{0},R); \\ \phi(\mathbf{y}), & \textit{ha } \mathbf{y} \in \partial\mathbb{B}(\mathbf{0},R) \end{cases}$$

függvény harmonikus $\operatorname{int}\mathbb{B}(\mathbf{0},R)$*-en és folytonos* $\mathbb{B}(\mathbf{0},R)$*-en.*

Dirichlet-probléma gömbben

Következmény. *Bármely $\phi \in C^0(\partial\mathbb{B}(\mathbf{0},R))$ esetén a*

$$\begin{aligned} \Delta u(\mathbf{x}) &= 0 && (\forall\, \mathbf{x} \in \operatorname{int}\mathbb{B}(\mathbf{0},R)); \\ u(\mathbf{x}) &= \phi(\mathbf{x}) && (\forall\, \mathbf{x} \in \partial\mathbb{B}(\mathbf{0},R)) \end{aligned}$$

Dirichlet-próblémának egyetlen $u \in C^2(\operatorname{int}\mathbb{B}(\mathbf{0},R)) \cap C^0(\mathbb{B}(\mathbf{0},R))$ megoldása van.

Fourier módszer $\mathbb{R}^2$-ben

Polárkoordinátákkal

$$\Delta u = \frac{\partial^2 u}{\partial r^2} + \frac{1}{r}\cdot\frac{\partial u}{\partial r} + \frac{1}{r^2}\cdot\frac{\partial^2 u}{\partial \phi^2}.$$

Keressük az $u(r,\phi) = R(r)\,\Phi(\phi)$ alakú megoldásokat.

Példa (forgásszimmetrikus eset). Ekkor $\Phi \equiv \mu \neq 0$ (a $\Phi \equiv 0$ eset trriviális). Ekkor

$$\begin{aligned} \Delta u = 0 &= \mu\left(R'' + \frac{R'}{r}\right); \\ r^2R'' + rR' &= 0; \\ R(r) &= a\ln r + b, \end{aligned}$$

ebből $u(r,\phi) = \hat{a}\ln r + \hat{b}$.

2.7. Dinamikus rendszerek egyensúlyi helyzeteinek, periodikus pályáinak stabilitása

A tételhez kapcsolódó anyagrészek megtalálhatóak Makay Géza: *Dinamikus rendszerek* című tárgyhoz készült jegyzetében [7].

Egy γ periodikus pálya *stabil*, ha γ minden U környezetéhez van olyan V környezete γ-nak, hogy V bármely pontjából indítva, a dinamikus rendszer U-ban marad. Egy γ periodikus pálya *aszimptotikusan stabil*, ha stabil és bármely $x \in V$-re az x-ből indított megoldás távolsága γ-tól 0-hoz tart az „idő múlásával".

Poincaré-leképezés

Lásd [7, 33–34. oldal]. A Poincaré-leképezés fixpontjai az egyenlet periodikus pályáinak felel meg. A Poincaré-leképezés fixpontja (aszimptotikusan) stabil akkor és csak akkor, ha a dinamikus rendszer azon pontjából indított zárt pályája (aszimptotikusan) stabil.

Ha γ az f periodikus pályája és a Poincaré-leképezés minden sajátértéke az egységkörön belül van, akkor a periodikus pálya aszimptotikusan stabil. A Poincaré-leképezés sajátértékei függetlenek a transzverzális választásától.

Orbitális stabilitás

Egy γ periodikus pálya *orbitálisan stabil*, ha γ minden U_1 nyílt környezetéhez van olyan U_2 környezete, hogy ha $x \in U_2$, akkor a dinamikus renszer az x-ből indítva U_1-ben marad. *Aszimptotikusan orbitálisan stabilitás* hasonlóan a korábbiakhoz.

Egy x pontnak T *aszimptotikus periódusa*, ha egy megoldás és a T-idővel vett eltoltjának a távolságának a határértéke 0.

Hartman – Grobman-tétel

Egy x fixpont *hiperbolikus*, ha az $f'(x)$ mátrixnak nincs 0 valós részű sajátértéke. Egy x fixpont *kritikus pont*, ha az $f'(x)$ mátrixnak van 0 valós részű sajátértéke.

A Hartman – Grobman-tételek [7, 52. oldalától] kezdődnek. Lényegében olyasmit állít, hogy fixpontok közelében egy adott dinamikus rendszerrel van topologikusan ekvivalens dinamikus rendszer, mely lineáris egyenletből származik.

2.8. Globális eredmények dinamikus rendszerek mozgásainak aszimptotikus viselkedéséről

A tételhez kapcsolódó anyagrészek megtalálhatóak Makay Géza: *Dinamikus rendszerek* című tárgyhoz készült jegyzetében [7].

Egy T *dinamikus rendszer* egy olyan leképezés, amely egy G félcsoport és egy X metrikus tér Descartes-szorzatáról képez a metrikus térre, és teljesülnek rá bizonyos tulajdonságok (lásd [7, 18. oldal]). Ha G csoport akkor T *invertálható dinamikus rendszer*. Ha G az egész számok halmaza vagy a pozitív egész számok halmaza, akkor a dinamikus rendszer *diszkrét*. Ha G a valós számok halmaza, vagy a pozitív félegyenes akkor T *folytonos* dinamikus rendszer.

Határpontok, határhalmazok

Lásd [7, 4. oldal].

Legyen $\xi \in D$ olyan pont hogy a belőle indított megoldás értelmezési tartománya tartalmazza a nemnegatív félegyenest. A $p \in D$ a ξ-ből indított megoldás ω*-határpontja*, ha létezik olyan t_k végtelenbe tartó sorozat, melyet a ξ-ből indított megoldásba írva a megoldás p-be tart. Az α*-határpontok* ugyanilyenek, csak a végtelent mindenhol mínusz végtelenre cseréljük. Ezek halmazai az α- és ω-*határhalmazok*. Bővebben, illetve a határhalmazok tulajdonságait lásd a jegyzeben.

Poincaré – Bendixson-tétel

Lásd [7, 40. oldal].

Ha f a dinamikus rendszert meghatározó függvény, és f folytonosan differenciálható az M értelmezési tartományán, $x \in M$, és az $\omega(x)$ határhalmaz nemüres, kompakt, összefüggő, és csak véges sok fixpontot tartalmaz akkor a következők egyike teljesül:

1. $\omega(x)$ egy fixpont;
2. $\omega(x)$ egy reguláris periodikus pálya;
3. $\omega(x)$ előáll véges sok fixpont és azokat egyértelmű módon összekötő pályák uniójaként.

Attraktorok

Lásd [7, 18–21. oldal].

Egy diszkrét dinamikus rendszer felírható egy f leképezés iteráltjaként.

A p n-periodikus pont *stabil halmaza* az *előre aszimptotikus pontjainak* a halmaza; *instabil halmaza* a *hátra assziptotikus pontjainak* a halmaza. A p n-periodikus pont *attraktor* ha stabil halmaza tartalmazza egy nyílt környezetét is, *repellor*, ha instabil halmaza tartalmazza egy nyílt környezetét is.

Attraktorok [6, 310. oldal] alapján: tekintsük az $\mathbf{x}' = f(\mathbf{x})$ differenciálegyenletet $\mathbb{R}^n$-ben, és legyen ϕ_t egy megoldás. Egy Λ halmaz *attraktor*, ha:

1. invariáns és kompakt;
2. létezik olyan Λ-t tartalmazó U halmaz, amelyre bármely $\mathbf{x} \in U$ esetén $\phi_t(\mathbf{x}) \in U$ bármely $t > 0$ esetén és $\bigcap_{t \geq 0} \phi_t(U) = \Lambda$;
3. Tetszőleges $\mathbf{y}_1, \mathbf{y}_2 \in \Lambda$ és U_1, U_2 nyílt környezetük esetén létezik olyan megoldás, ami U_1-ből indul és áthalad U_2-n.

Strukturális stabilitás

Lásd [7, 26. oldal].

Egy f dinamikus rendszer *C^r-strukturálisan stabil*, ha létezik olyan $\epsilon > 0$, hogy bármely g dinamikus rendszerre, melynek C^r távolsága f-től kisebb, mint ϵ, f és g topologikusan ekvivalensek. Fixpont C^r-strukturális stabilitása hasonlóan, a fixpont egy környezetére kell a topologikus ekvivalencia.

Kaotikus dinamika

Lásd [7, 30. oldal].

Egy $f\colon M \to M$ dinamikus rendszer *kaotikusan viselkedik*, ha f folytonos, M végtelen halmaz, f topologikusan tranzitív és f periodikus pályái sűrűn vannak M-ben. Ha f kaotikus, akkor érzékenyen függ a kezdeti feltételektől.

Hamilton-rendszerek

Lásd [6, 207. oldal]

$$x' = H'_y(x, y);$$
$$y' = H'_x(x, y),$$

ahol H C^∞ függvény a *Hamilton-függvény*.

Azért fontosak, mert a H függvény *első integrál*, vagyis konstans a megoldások mentén.

2.9. A bonyolultságelmélet alapjai

A tételhez kapcsolódó anyagrészek megtalálhatóak Hajnal Péter: *Algoritmusok és bonyolultságelmélet* [5] című kurzusához kapcsolódó honlapon.

Turing-gépek

A Turing-gép definíciójához lásd [5, *Kiszámíthatóság, Turing-gép, alapfogalmak*]. Az f függvényt *kiszámítja* a T Turing-gép, ha minden lehetséges ω input esetén a gép véges lépésben leáll és az output $f(\omega)$.

Az *eldöntő Turing-gép* a Stop állapot helyett Elvet és Elfogad állapotokkal rendelkezik. Egy eldöntő Turing-gép *eldönti* az L nyelvet, ha minden L-beli inputra véges lépsben Elfogad állapottal áll meg, míg nem L-beli inputra Elvet állapottal áll le. Egy Turing-gép *felsorolja* az L nyelvet,

ha minden L-beli inputra ELFOGAD-dal leáll és minden nem L-beli inputra *nem* áll le. Felsorolható nyelvek osztálya $\mathcal{S}$, Eldönthető nyelvek osztálya $\mathcal{D}$, $\mathcal{S}$ tartalmazza $\mathcal{D}$-t. A következőket lásd [5, *Bonyolultsági osztályok, Turing-gép fogalmának változatai...*].

Turing-gép *időigénye* egy ω inputon ℓ, ha futása az ℓ-ik konfigurációban kerül először STOP állapotba. Turing-gép *tárigénye* egy ω inputon s, ha munkaszalag legnagyobb felhasznált mezőjének indexe s. A T turing gép eleme a $\mathrm{TIME}(t(n))$ halmaznak, ha időigénye tetszőleges ω input esetén kisebb, mint $t(|\omega|)$. Ugyanígy $\mathrm{SPACE}(t(n))$ halmaz.

Egy L eldönthető nyelv eleme a $\mathrm{TIME}(t(n))$ osztálynak, ha létezik olyan T Turing-gép, ami eldönti L-et és T eleme a $\mathrm{TIME}(t(n))$ osztálynak. $\mathrm{SPACE}(t(n))$-re hasonlóan. Ezek alapján definiálhatjuk a P, EXP, PSPACE, EXPSPACE, L osztályokat.

Nemdeterminisztikus Turing-gép

Lásd [5, *Nem-determinizmus, Bonyolultsági osztályok...*].

Az input és a munkaszalag között van egy plusz szalag is a *tanúszalag*. Ez csak olvasható és a fej csak jobbra tud rajta mozogni. Az ω inputot pontosan akkor fogadja el a nemdeterminisztikus Turing-gép, ha van olyan tanúszalag tartalom amire ELFOGAD állpotba jut. ELVET állapot esetén sem feltétlen rossz az input. Az igazi elvetés akkor történik, ha minden tanúszalag-tartalomra ELVET állapotba jutunk.

Ezek alapján bevezethetjük a nemdeterminisztikus osztályokat: NP, NEXP, NL, NPSPACE, NEXPSPACE. A determinisztikus osztályok zártak a komplementálásra, de a nemdeterminisztikus osztályok nem feltétlenül. Ezek alapján definiálhatjuk a co-NP, co-NL, stb. osztályokat. Felírhatunk egy tartalmazási láncot. Növekvő sorban: L, NL, P, NP, PSPACE, NPSPACE, EXPSPACE, NEXPSPACE

Kiszámíthatatlan problémák

Lásd [5, *Példák*].

Megállás (Turing-tétel). Adott T Turing-gép és ω input esetén el kell döntenünk, hogy T leáll-e ω-n. MEGÁLLÁS eleme $\mathcal{S}$-nek, de nem eleme $\mathcal{D}$-nek.

Post-probléma. Adott véges ábécé, a szavakból dominókat készítünk (alsó és a felső részén is egy szó van.) és minden dominóból végtelen sokat. Ki tudunk-e rakni a dominóinkból egy sort úgy, hogy az alsó és felső részen is ugyanazt tudjuk összeolvasni? POST nem eleme $\mathcal{D}$-nek.

Szóprobléma. Az input egy G multiplikatív csoport (valahogyan kódolva), és két, a generátorhalmazának elemeiből készített szó. A kérdés, hogy hogy a két szó ugyanazt a csoportelemet reprezentálja-e? SZÓPROBLÉMA nem eleme $\mathcal{D}$-nek.

Dipohantosz (Hilbert X. problémája). Az input egy egész együtthatós polinom, kérdés, van-e egész gyöke. DIPOHANTOSZ nem eleme $\mathcal{D}$-nek.

Homeomorf. Inputja két topologikus tér, el kell dönteni, hogy hoemomorfak-e. HOMEOMORF nem eleme $\mathcal{D}$-nek.

Redukció, teljesség

Lásd [5, *Redukciók, teljes nyelvek...*].

Legyen L, L' két nyelv, C bonyolultsági osztály. L *redukálható* L'-re C-ben, ha létezik olyan C bonyolultságú R kiszámító Turing-gép, hogy ha $\omega \in L$ akkor $\omega' \in L'$, ahol ω' az ω-ból R által kiszámolt output.

Az L' nyelv *teljes* a C osztályban az R bonyolultságú redukcióra nézve, ha $L' \in C$ és bármely $L \in C$-re L R-redukálható L'-re. P-teljesség L-teljesség, stb.

Cook – Levin-tétel

Lásd [5, *P-teljes és NP-teljes problémák, Cook-Levin tétel*].

A SAT-probléma NP-teljes. SAT-probléma: adott CNF kielégíthető-e?
További NP-teljes problémák:

3-színezhetőség. Síkgráf 3-színezhetősége.

Független csúcshalmaz. Adott G gráf és k egész esetén, van-e G-ben k pontú független ponthalmaz?

Klikk, lefogó ponthalmaz. Hasonlóan, mint a független csúcshalmaz.

Hamilton. Adott G gráf rendelkezik-e Hamilton-körrel?

Max-Cut. Adott G gráf, k egész, van-e G-ben legalább k elemű vágás?

Véletlen Turing-gépek

Lásd [5, *Véletlen számítások, bonyolultsági osztályok*].

Egy T Turing gépet *véletlen Turing-gépnek* nevezünk, ha rendelkezik plusz egy véletlen szalaggal, amelyen véletlen számok szerepelnek. A szalagon lévő fej csak jobbra lépni és olvasni képes. Az input és a véletlen szalag tartalmának ismeretében a futás determinisztikus, azonban ha csak az inputot ismerjük, a futás szerteágazó lehet.

Egy L nyelv eleme BPP-nek, ha létezik olyan polinom idejű T Turing-gép, ami legalább $\frac{2}{3}$ valószínűséggel jó döntést hoz.

Egy L nyelv eleme RP-nek, ha létezik olyan polinom idejű T Turing-gép, ami legalább $\frac{1}{2}$ valószínűséggel dönt jól, ha az input L-beli, viszont biztosan jó döntést hoz, ha az input nem L-beli.

2.10. Hibajelző és -javító kódolások

A tételhez kapcsolódó anyagrészek egy része megtalálhatóak a Czédli Gábor: *Boole-függvények* [3] című könyvének 3. fejezetében.

Alapfogalmak és célok

Célunk olyan a kételemű test (vagy véges test) feletti n-dimenziós vektortérből az m-dimenziós vektortérbe $n < m$ menő injektív leképezések – *kódok* – konstrukciója *bináris szimmetrikus csatorna* mellett (bitek p valószínűségel „fordulnak át”), melyek hatékonyan *dekódolhatók* (az eredeti üzenetet próbáljuk meg rekonstruálni). Dekódolás lehet *hibajelző* vagy *hibajavító*. A szokásos modell: feladó – kódolás – csatorna (hiba) – dekódolás – fogadó.

Ha egy kód (a leképezés képtere) lineáris altér, akkor a C kódot *lineáris kódnak* nevezzük. A $\mathbf{G}$ $k \times n$-es mátrixot C *generátormátrixának* nevezzük, ha sorai lineárisan függetlenek és kifeszítik C-t. Egy $\mathbf{G}$ generátormátrixot *standard generátormátrixnak* nevezünk, ha

$$\mathbf{G} = \begin{bmatrix} \mathbf{I}_k & \mathbf{B} \end{bmatrix}$$

alakú (ekkor C dimenziója k). Kódoláselméleti kontextusban sorvektorokkal dolgozunk. Két kódot *ekvivalensnek* nevezünk, ha létezik a koordinátáknak olyan permutációja, amellyel a két kód egymásba vihető. Bármely lineáris kód ekvivalens egy olyan lineáris kóddal, amelynek van standard generátormátrixa.

Paritásellenőrző mátrix

Egy lineáris kód *duálisának* nevezzük a rá merőleges alteret, jelölésben $C^\perp$. Ha $C \leq \mathbb{F}_q^n$, akkor $\dim C + \dim C^\perp = n$, valamint $\left(C^\perp\right)^\perp = C$. A $C^\perp$ lineáris kód $\mathbf{H}$ generátormátrixát a C kód *paritásellenőrző mátrixának* nevezzük. Ekkor

$$C = \left\{ \mathbf{x} \in \mathbb{F}_q^n \colon \mathbf{H}\mathbf{x}^{\mathrm{T}} = \mathbf{0}^{\mathrm{T}} \right\}.$$

Ha $\mathbf{G} = \begin{bmatrix}\mathbf{I}_k & \mathbf{B}\end{bmatrix}$ a C kód generátormátrixa, akkor $\mathbf{H} = \begin{bmatrix}-\mathbf{B}^{\mathrm{T}} & \mathbf{I}_{n-k}\end{bmatrix}$ paritásellenőrző mátrixa C-nek. Ha C lineáris $[n,k]$-kód, akkor duálisa lineáris $[n,n-k]$-kód.

Egy kód *minimumtávolsága* (a kódszavak közötti legkisebb távolság) pontosan akkor lesz legalább $t+1$, ha a paritásellenőrző mátrixnak bármely t oszlopa lineárisan független.

Hamming-kódok

A kételemű test feletti r-ik Hamming-kódokat vizsgáljuk. Tekintsük $\mathbb{F}_2^r$ egydimenziós altereit (ezekből 2^r-1 van), minden egyenesről tekintsük azt a pontot, amelyik nem az origó, és ezeket mint oszlopvektorokat írjuk bele a $\mathbf{H}_r$ mátrixba (most speciálisan 1-től 2^r-1-ig a számokat bináris alakban), és tekintsük azt a kódot, melynek paritásellenőrző mátrixa $\mathbf{H}_r$: ez az *r-edik bináris Hamming-kód*.

Ez a kód egy lineáris $[n,n-r]$-kód ($n=2^r-1$), és minimumtávolsága $d=3$, sőt *perfekt* (a kódszavak köré írt $\frac{d-1}{2}$ sugarú gömbök lefedik $\mathbb{F}_2^n$-t). Hibajezés és -javítás könnyű: *tünet* (vagy *szindróma*: $\mathbf{H}_r\mathbf{x}^{\mathrm{T}}$) segítségével.

Reed – Muller-kódok

Legyen

$$\mathbf{G}_r = \begin{bmatrix}\mathbf{1}_{2^r-1} & 1\\ \mathbf{H}_r & \mathbf{0}_r^{\mathrm{T}}\end{bmatrix},$$

ekkor a $\mathbf{G}_r$ mátrix által generált kódot *r-ik Reed – Muller-kódnak* nevezzük. Ez egy lineáris $[2^r, r+1]$-kód 2^{r-1} minimumtávolsággal.

Megemlíthető a *bináris Golay-kód*, amely egy *önduális* kód.

Ciklikus kód

Egy lineáris $C \leq \mathbb{F}_q^n$ kódot *ciklikusnak* nevezünk, ha bármely kódszó esetén annak „ciklikus elforgatottja" is eleme a kódnak (a koordináták „körbepermutálására" zárt a kód).

Az $\mathbb{F}_q[x]/(x^n-1)$ faktorgyűrű ideáljai éppen a ciklikus kódok. Ez a gyűrű főideálgyűrű, és minden idál előáll egy alkalmas minimális fokszámú főpolinom generátumaként, ezt nevezzük a megfelelő kód *generátorpolinomjának*. Ha generátorpolinom foka k, akkor a kapott ciklikus kód egy lineáris $[n,n-k]$-kód.

Ciklikus kódok esetén a kódolás polinomszorzás, a hibajelzés polinomosztás (a generátorpolinommal, lásd [3, 39. oldal]). Ilyen kódoknál a *hibacsapdázó algoritmus* segítségével a *csomós hibák* jól javíthatók. Megemlíthető: *kódátfűzés* CD-k esetében.

Véges testek és BCH-kódolás

Bose és Chadbury, illetve tőlük függetlenül Hocquenghem megfelelő kódokat fedeztek fel közepes kódhossz ($n=$ néhány száz) esetére, az ún. BCH-kódokat (lásd a BCH-kódok alaptételét [3, 3.6. tétel, 36. oldal])

Legyen f egy r-edfokú primitív polinom (lásd [3, 35. oldal]) $\mathbb{F}_2$ felett, és legyen $\alpha = x+(f) \in \in \mathbb{F}_{2^r}$. Tekintsük α-nak $d-1$ darab egymást követő hatványának minimálpolinomjait, majd vegyük a legkisebb közös többszörösüket, g-t: g lesz a kód *generátorpolinomja*. Ekkor a kódolás (megfelelő paraméterek mellett, lásd [3, 3.7. definíció, 38. oldal]) a g-vel való szorzást lesz a BCH-kód kódolása. A BCH-kód lineáris, és minimumtávolsága (a kódszavak közötti legkisebb távolság) legalább d.

A leggyakrabban használt a $d=7$ és $r=8$ esetén egy $[255, 231]$ típusú, (legalább) 6-hibajelző BCH-kódolás.

Reed – Solomon-kód

Legyen β egy nemnulla eleme $\mathbb{F}_q$-nak, jelölje n a β elem *multiplikatív rendjét* (a legkisebb pozitív egészet, amire β-t emelve 1-et kapunk). Legyen $d>2$, $a \geq 0$ és $f(x) = x^n - 1$,

$$g(x) = \prod_{i=1}^{d-1} \left(x - \beta^{a+i}\right)$$

a kód generátorpolinomja (foka $d-1$). Ezt a kódot *Reed – Solomon-kódnak* nevezzük, ez egy ciklikus $[n, n-d+1]$-kód, melynek minimumtávolsága d.

A leggyakrabban használt az $\mathbb{F}_{2^8}$ feletti $[255, 223]$ típusú Reed – Solomon-kód.

2.11. Sűrűség és mérték síkbeli geometriai elemek halmazain, hossz- és területformulák

A tételhez kapcsolódó anyagrészek megtalálhatóak a Luis A. Santaló: *Integral Geometry and Geometric Probability* [12] című könyv I. részében.

Motivációként elhangozhat a Bertrand-paradoxon: *mennyi a valószínűsége, hogy egy szabályos háromszög köré írt körben véletlenül választott húr hossza nagyobb a háromszög oldalánál?* Legalább háromféleképpen közelíthetjük meg a problémát: megválaszthatjuk a húr két végpontját, ekkor a valószínűség $\frac{1}{3}$; választhatjuk a normálvektorának (origó a kör középpontja) szögét, majd távolságát az origótól, ekkor a valószínűség $\frac{1}{2}$; illetve választhatjuk a húr középpontját véletlenszerűen, ekkor a valószínűség $\frac{1}{4}$ (az $\frac{1}{2}$ sugarú koncentrikus körön kívül bármelyik pont megfelelő lesz).

Sűrűség és mérték pont- és egyeneshalmazokon, elemi integrálformulák

Lásd [12, 2. fejezet, 1. szakasz].

Integrálgeometriai kontextusban olyan mértéket (sűrűséget) keresünk, amely *mozgásinvariáns*. Szokásosan (x, y) Descartes-koordinátákat alkalmazva a síkon egy mozgás a következőképpen transzformál:

$$\begin{aligned} x' &= x\cos\theta - y\sin\theta + a; \\ y' &= x\cos\theta + y\sin\theta + b. \end{aligned}$$

Tehát olyan $\mu(X) = \int_X f(x,y)\,\mathrm{d}x \wedge \mathrm{d}y$ mértéket keresünk, amely bármely a fenti alakú mozgásra invariáns. Ebből következik, hogy $f(x,y) = f(x',y')$ bármely mozgásra, mivel tetszőleges két pont mozgással átvihető egymásba a síkon, így adódik, hogy f konstans (speciálisan választhatjuk 1-nek).

Definíció (sűrűség ponthalmazokon)**.** A síkon *ponthalmazok sűrűsége*

$$\mathrm{d}P = \mathrm{d}x \wedge \mathrm{d}y,$$

mértéke pedig a fenti sűrűség integrálja a halmazon.

Hasonlóan független pont-n-esek halmazának sűrűsége $\mathrm{d}P_1 \wedge \mathrm{d}P_2 \wedge \ldots \wedge \mathrm{d}P_n$ (konstansszorzó erejéig egyértelmű). Áttérés másik (Descartes-féléből származtatott) koordináta-rendszerre Jacobi-mátrixszal.

Az egyenesek halmazain mozgásinvariánsmértéket kapunk, ha az egyeneseket a normálvektoruk x-tengellyel vett szögével – ϕ – és az origótól vett távolságukkal – p – paraméterezzük: $\mathrm{d}e = \mathrm{d}p \wedge \mathrm{d}\phi$. Ebből rögtön adódik, hogy tetszőleges K konvex halmaz esetén (lásd [12, 29–30. oldal])

$$\begin{aligned} \int_{e\cap K\neq\emptyset} |e\cap K|\,\mathrm{d}e &= \pi T(K); \\ \mu(e\colon e\cap K\neq\emptyset) = \int_{e\cap K\neq\emptyset} \mathrm{d}e &= L(K), \end{aligned}$$

azaz a korlátos konvex K halmazt metsző egyenesek mértéke éppen K kerülete. Így egy K-t metsző egyenes K-ba eső részének hosszána várható értéke $\mathbb{E}(\sigma) = \pi\frac{T(K)}{L(K)}$.

Ha C egy szakaszonként differenciálható görbe, akkor véletlen egyenesek C-vel vett metszéspontjai számának integrálja éppen C hosszának kétszerese: $\int n\,\mathrm{d}e = 2L$ (Crofton, lásd [12, 31. oldal]).

Pont- és egyenespárok halmazainak mértéke

Pontpárok sűrűségét láttuk: $\mathrm{d}P_1 \wedge \mathrm{d}P_2$, azonban áttérhetünk a következő paraméterezésre: vegyük a két pontot összekötő egyenest – e: p, ϕ – a legközelebbi pontját az origóhóz, és a két pont távolságát – t_1, t_2 – ettől a ponttól. Ekkor (lásd [12, 46. oldal])

$$\mathrm{d}P_1 \wedge \mathrm{d}P_2 = |t_2 - t_1| \, \mathrm{d}e \wedge \mathrm{d}t_1 \wedge \mathrm{d}t_2.$$

Ebből levezethető a következő:

$$\mathbb{E}\left(|\overline{\mathbf{p}_1\mathbf{p}_2}|\right) = \frac{1}{6T^2(K)} \int_{e \cap K \neq \emptyset} \sigma^4 \, \mathrm{d}e.$$

Legyen e_1 és e_2 két egyenes, melyek P-ben metszik egymást és az x tengely pozitív irányával rendre α_1, α_2 szöget zárnak be. Ekkor (lásd [12, 49. oldal])

$$\mathrm{d}e_1 \wedge \mathrm{d}e_2 = |\sin(\alpha_2 - \alpha_1)| \, \mathrm{d}P \wedge \mathrm{d}\alpha_1 \wedge \mathrm{d}\alpha_2.$$

Ebből, ha K korlátos és konvex, akkor véve a K-t metsző egyenespárok mértékéből adódik, hogy ha ω jelöli az egy pontból K-hoz húzott érintők bezárt szögét, akkor

$$\int_{P \notin K} (\omega - \sin\omega) \, \mathrm{d}P = \frac{1}{2} L^2(K) - \pi T(K). \qquad \text{(Crofton)}$$

Mivel $\mu(e_1 \cap e_2 \in K) = 2\pi T(K)$, ebből $\mathbb{P}(e_1 \cap e_2 \in K) = \frac{2\pi T(K)}{L^2(K)}$ – ez legfeljebb $\frac{1}{2}$ (kör esetén vétetik fel), ez az *izoperimetrikus probléma*.

Buffon-féle tűprobléma

Tekintsük egy párhuzamos, egymástól egységnyi távolságra lévő egyenessereget a síkon. Mennyi a valószínűsége, hogy egy $\ell < 1$ hosszú „tűt” a síkra ejtve (matematikai módon), az metszi valamelyik egyenest?

Világos, hogy 1 átmérőjű kört legfeljebb egy egyenes metszhet. Legyen ez a kör és benne a tű rögzített! Ekkor a korábbiak szerint a keresett valószínűség $\mathbb{P}(\ell \cap e \neq \emptyset) = \frac{2\ell}{\pi}$. A feladatnak léteznek különböző általánosításai, például sávokkal és konvex lemezekkel.

Konvex halmazok támaszfüggvényeinek integráljai

Legyen $p(\phi)$ a K konvex halmaz *támaszfüggvénye* (lásd [12, 1. fejezet, 2. szakasz, 3–4. oldal]). Ekkor

$$L(K) = \int_0^{2\pi} p(\phi) \, \mathrm{d}\phi;$$
$$T(K) = \frac{1}{2} \int_0^{2\pi} p\left(p + p''\right) \mathrm{d}\phi = \frac{1}{2} \int_0^{2\pi} \left(p^2 - \left(p'\right)^2\right) \mathrm{d}\phi.$$

Sylvester-probléma

Lásd [12, 4. fejezet, 5. szakasz, 63–65. oldal].

Mi a valószínűsége, hogy egy K konvex halmazból 4 pontot véletlenszerűen választva a konvex burkuk négyszög?

Ez a valószínűség

$$p = 1 - 4\mathbb{P}\left(\begin{array}{c}\text{az egyik pont a másik három által}\\ \text{meghatározott háromszögben van}\end{array}\right) = 1 - 4\frac{T_2}{T^4(K)};$$
$$T_2 = \iiint_{P_0, P_1, P_2, \in K} T(\triangle_{P_0P_1P_2}) \, \mathrm{d}P_0 \wedge \mathrm{d}P_1 \wedge \mathrm{d}P_2.$$

Háromszög esetén $T_2 = \frac{T^4(K)}{12}$, így $p = \frac{2}{3}$, míg kör esetén $p = 1 - \frac{35}{12\pi^2}$.

2.12. Differenciálformák, kinematikai sűrűség és mérték

A tételhez kapcsolódó anyagrészek megtalálhatóak a Luis A. Santaló: *Integral Geometry and Geometric Probability* [12] című könyv I. részében.

Differenciálformák euklideszi tereken – a síkon

Lásd [12, 6. fejezet, 2. szakasz, 82–84. oldal].

A mozgásokon vett *elsőrendű differenciálformának* (vagy 1-formának) nevezünk bármely

$$\omega(u) = \alpha(u)\,\mathrm{d}a + \beta(u)\,\mathrm{d}b + \gamma(u)\,\mathrm{d}\theta,$$

ahol az α, β, γ függvények C^∞-függvények a mozgások terén, azaz végtelen sokszor folytonosan differenciálhatók az u mozgás a, b, θ koordinátáiban.

Kiszámolható, hogy mely 1-formák alkotnak „bázist” $(\omega_1, \omega_2, \omega_3)$ a *bal eltolásokon* (először θ_0-szöggel forgatunk, utána alkalmazzuk u-t) invariáns formákon. Hasonlóan a kiszámolható, hogy mely 1-formák alkotnak „bázist” $\left(\omega^1, \omega^2, \omega^3\right)$ a *jobb eltolásokon* (először u-t alkamazzuk, mad eltolunk (a, b)-t) invariáns formákon.

Ekkor a következő 3-formára (lásd [12, 6. fejezet, 3. szakasz, 85. oldal]):

$$\omega_1 \wedge \omega_2 \wedge \omega_3 = \mathrm{d}a \wedge \mathrm{d}b \wedge \mathrm{d}\theta = \mathrm{d}K = \mathrm{d}a \wedge \mathrm{d}b \wedge \mathrm{d}\theta = \omega^1 \wedge \omega^2 \wedge \omega^3;$$
$$\mathrm{d}K\left(u^{-1}\right) = -\mathrm{d}K(u),$$

de mivel sűrűségnél abszolútértéket veszünk, ezért a $\mathrm{d}K$ 3-forma invariáns a bal és a jobb eltolásokon is.

Kinematikus mérték

Egy síkbeli mozgást paraméterezhetünk a(z origó körüli) forgatás szögével – θ –, illetve az eltolásvektor koordinátáival – (a, b). A síkbeli mozgások *kinematikus sűrűsége* $\mathrm{d}a \wedge \mathrm{d}b \wedge \mathrm{d}\theta$ (térfogat $\mathbb{R}^2 \times [0, 2\pi)$-n), mivel ez a mérték invariáns, azaz, ha H mozgások egy halmaza, akkor $\mu(uH) = \mu(H) = \mu(Hu)$ (komplexusszorzás), illetve $\mu(H) = \mu\left(H^{-1}\right)$ (elemenkénti inverz). Nyilván a mérték a sűrűség integrálja lesz.

Áttérhetünk egy másik ekvivalens kinematikus sűrűségre is: Tekintsük az x-tengely képét, az e^* irányított egyenest – $\mathrm{d}e^* = \mathrm{d}p \wedge \mathrm{d}\phi$ – valamint e^* „talppontjának” és az origó képének a távolságát – t –, ekkor $\mathrm{d}a \wedge \mathrm{d}b \wedge \mathrm{d}\theta = \mathrm{d}K = \mathrm{d}e^* \wedge \mathrm{d}t$.

A térben a mozgások tengelyes forgások (3×3-as, 1-determinánsú mátrixok – $\mathrm{SO}(3)$) és eltolások – $\mathbf{t}$ – szorzataként állnak elő. A forgatás $\mathbf{v}$ tengelye, és α szögéről áttérve $\mathbf{w}$-ra és θ-ra a $\mathrm{d}\mathbf{w} \wedge \mathrm{d}\theta \wedge \mathrm{d}\mathbf{t}$ sűrűség lesz a *kinematikus sűrűség* a térbeli mozgásokon.

Mérték szakaszok halmazain

Lásd [12, 6. fejezet, 4. szakasz, 89–90. oldal].

Legyen K irányított szakasz ℓ hosszal, K_0 rögzített konvex lemez. A K_0-t metsző K-val egybevágó (mozgásokkal kapható) szakaszok mértéke:

$$\int_{K \cap K_0 \neq \emptyset} \mathrm{d}K = \int_{K \cap K_0 \neq \emptyset} \mathrm{d}e^* \wedge \mathrm{d}t = \int_{e \cap K_0 \neq \emptyset} (\sigma + \ell)\,\mathrm{d}e^* = 2\pi T(K_0) + 2\ell L(K_0).$$

Konvex alakzatot metsző konvex alakzatok halmazainak mértéke

Lásd [12, 6. fejezet, 5. szakasz, 93–95. oldal]:

$$\mu(K_1 \colon K_1 \cap K_0 \neq \emptyset) = \int_{K_1 \cap K_0 \neq \emptyset} \mathrm{d}K_1 = 2\pi\left(T(K_1) + T(K_0)\right) + L(K_0)\,L(K_1).$$

Poincaré-formula

Lásd [12, 7. fejezet, 2. szakasz, 111. oldal].

Legyenek Γ_0, Γ_1 szakaszonként sima görbék a síkon. Ekkor

$$\int_{\Gamma_0 \cap \Gamma_1 \neq \emptyset} n \, \mathrm{d}K_1 = 4 L_0 L_1, \qquad \text{(Poincaré)}$$

ahol bal oldalon Γ_1-nek Γ_0-t metsző példányainak mértéke áll. Az integrandusban szereplő n a *metszési szám*, L_0, L_1 a megfelelő görbék hosszai. A számolás természetes paraméterezésre, és az ezzel kapcsolatos mértékre történő áttéréssel megy.

Blaschke alapformulája

Lásd [12, 7. fejezet, 4. szakasz, 114. oldal].

Legyen D_0, D_1 két tartomány (összefüggő és nyílt), szakaszonként sima, irányított, nem önátmetsző görbékkel határolt. Legyen c_0, c_1 a megfelelő tartományok *teljes görbülete* (a határgörbék görbületei integráljainak összege), míg $c_{0\,1}$ legyen a $D_0 \cap D_1$ tartomány teljes görbülete. Ekkor

$$\int_{D_0 \cap D_1 \neq \emptyset} c_{0\,1} \, \mathrm{d}K_1 = 2\pi \left(T\left(D_0\right) c_1 + T\left(D_1\right) c_0 + L\left(D_0\right) L\left(D_1\right) \right). \qquad \text{(Blaschke)}$$

A. függelék

Tudáselemek

Gráfelmélet: összefüggőség, színezések. Fák összeszámlálása, gráfok magasabb fokú összefüggősége, MENGER tételei, élszínezések, Vizing-tétel, csúcsszínezések, HAJÓS tétele, nagy derékbőségű, nagy kromatikus számú gráfok.

Gráfelmélet: párosítások, síkgráfok. Párosítási algoritmusok és gráfelméleti következményeik, síkgráfok, Kuratowski-tétel, Wagner-tétel, gráfok metszési száma.

Gröbner-bázisok és alkalmazásaik. HILBERT bázistétele, Galois-kapcsolat, radikálideálok, varietások, *Hilbert Nullstellensatz*, redukciós eljárás, ideálok Gröbner-bázisai, Buchberger-algoritmus, minimális és redukált Gröbner-bázisok, tartalmazási probléma, algebrailag zárt test feletti egyenletrendszerek megoldhatósága, véges varietások meghatározása, minimálpolinom-keresés, gráfszínezési probléma.

Matematikai titkosírások. Alapfogalmak és célok, nyilvános kulcsú titkosírás, RSA, prímtesztek: Soloway – Strassen, Miller – Rabin, AKS; a diszkrét logaritmus és alkalmazásai: Diffie – Hellman-kulcsváltás, Massey – Omura-rejtjelrendszer.

Többváltozós és vektorértékű függvények. Többszörös integrál, vonalintegrál, felületi integrál, Green-tétel, Gauss-tétel, Stokes-tétel, az integrálszámítás fizikai és műszaki alkalmazásai.

Fourier-sorok, ortogonális polinomok, sorfejtések. Trigonometrikus és ortogonális polinomsorok konvergenciája, Fourier-transzformált, Laplace-transzformált.

Közönséges differenciálegyenletek és elsőrendű parciális differenciálegyenletek. Létezés, egyértelműség, stabilitás, megmaradási törvények, egy- és többlépéses numerikus módszerek, a CFL-feltétel.

Többdimenziós normális eloszlású vektorok statisztikai analízise. Wishart-eloszlás, paraméterbecslés, hipotézisvizsgálat.

Lineáris regresszió. Véletlen változó lineáris közelítése véletlen változók lineáris kombinációjával, a lineáris modell: legkisebb négyzetek módszere, varianciaanalízis.

Kontingenciatáblák elemzése. Korrespondenciaanalízis, információelméleti módszerek.

Diszkrét idejű Markov-láncok. Definíció, átmenetvalószínűség, példák diszkrét idejű Markov-láncokra, a Markov-tulajdonság, a Chapman – Kolmogorov-egyenletek és az erős Markov-tulajdonság, Markov-láncok állapotai és osztályai, a szolidaritási tétel, Markov-láncok invariáns eloszlásai, a periodikus osztályok jellemzése, elérési idők, elnyelési valószínűségek, a bolyongás egy és magasabb dimenzióban, PÓLYA tétele, a játékos csődje probléma.

Folytonos idejű Markov-láncok. Felújítási folyamatok, az elemi felújítási tétel és a felújítási egyenlet, az infinitezimális generátor és Kolmogorov egyenletei, folytonos idejű Markov-láncok ekvivalens leírásai, állapotok, osztályok és invariáns eloszlás folytonos időben, a Poisson-folyamat és tulajdonságai.

Sztochasztikus folyamatok alapfogalmai. Definíció, típusok, példák, véges dimenziós eloszlások, a Kolmogorov-egzisztenciatétel, sztochasztikus folyamatok folytonossága és modifikációi, Gauss-folyamatok, a Wiener-folyamat és a Brown-híd, a Wiener-folyamat tulajdonságai: differenciálhatóság, kvadratikus variancia, iterált logaritmus tétel, tükrözési elv; a részletösszeg folyamat és az empirikus folyamat eloszlásbeli konvergenciája.

Optimalizálási eljárások. Optimalizálás alapfeladata és speciális esetei, Lagrange-módszer, Karush – Kuhn – Tucker-tétel, szimplex módszer, belsőpontos algoritmusok az LP feladat és SDP feladat problémákra, súlyozott párosítási probléma, az LP feladat és SDP feladat kombinatorikai alkalmazásai, egészértékű programozás, dinamikus programozás, korlátozás és szétválasztás módszerek alkalmazásai, gyakorlati problémák.

Mátrixok sajátértékeinek meghatározása. Mátrixok trianguláris felbontása, ortogonális triangularizáció, az LR-, QR- és R^HR algoritmus.

Mátrixok általánosított inverze. Kiszámítás rangfaktorizációval, ortogonális triangularizációval és particionálással, lineáris egyenletrendszerek vizsgálata.

Periodikus függvények diszkrét négyzetes közelítése. DFT, IDFT, FFT, számsorozatok konvolúciója.

A hullámegyenlet. Húr és membránok rezgései, d'Alambert-formula, hullámterjedés páros és páratlan dimenzióban, a leereszkedés módszere, Duhamel-elv, Fourier-módszer, a megoldások simasága, numerikus módszerek.

A hővezetés egyenlete. Maximum-minimum-elv, Cauchy-probléma megoldása, Poisson-integrál, a megoldások simasága, numerikus módszerek.

A Laplace-egyenlet. Harmonikus függvények, Green-függvények, Dirichlet-probléma gömbben, Poisson-formula, Dirichlet- és Neumann-problémák, Fourier-módszer, numerikus módszerek.

Dinamikus rendszerek egyensúlyi helyzeteinek, periodikus pályáinak stabilitása. Lokális invariáns sokaságok egyensúlyi helyzet környezetében, nyeregpont-tulajdonság, Grobman – Hartman-tétel, stabilitási eredmények, orbitális stabilitás, Poincaré-leképezések.

Globális eredmények dinamikus rendszerek mozgásainak aszimptotikus viselkedéséről. Limeszhalmazok, a Poincaré – Bendixson-tétel, attraktorok, strukturális stabilitás, generikus tulajdonságok, Hamilton-egyenletek, kaotikus dinamika.

A bonyolultságelmélet alapjai. Kiszámíthatóság, Turing-gépek, példák nem kiszámítható problémákra, nemdeterminisztikus, véletlen Turing-gépek, bonyolultsági osztályok és viszonyaik, Cook – Levin-tétel, NP-teljes problémák, nevezetes megoldatlan kérdések.

Hibajelző és -javító kódolások. Alapfogalmak és célok, véges testek és BCH-kódolás, paritásellenőrző mátrix, ciklikus kód, néhány konkrét kód: Hamming, Reed – Muller, Reed – Solomon.

Sűrűség és mérték síkbeli geometriai elemek halmazain, hossz- és területformulák. Sűrűség és mérték pont- és egyeneshalmazokon, pontpárok és egyenespárok halmazain, elemi integrálformulák hosszra, területre, szögekre (Crofton, stb.), Buffon-féle tűprobléma, konvex halmazok radiális és támaszfüggvényének integráljai, Sylvester-probléma véletlen pontnégyesek konvex burkáról.

Differenciálformák, kinematikai sűrűség és mérték. Differenciálformák euklidészi tereken, kinematikus mérték, mérték szakaszok és háromszögek halmazain, Poincaré-formula, Blaschke alapformulája, konvex alakzatot metsző konvex alakzatok halmazainak mértéke.

Irodalomjegyzék

[1] Benke János – Szűcs Gábor: Sztochasztikus folyamatok, 2016.
URL http://www.math.u-szeged.hu/~szucsg/oktatas/sztochfoly_slides.pdf.

[2] Bolla Marianna – Krámli András: *Statisztikai következtetések elmélete*. Budapest, 2012, Typotex.

[3] Czédli Gábor: *Boole-függvények*. Szeged, 2009, Polygon.

[4] Hajnal Péter: Diszkrét matematika, 2013.
URL http://www.math.u-szeged.hu/~hajnal/courses/MSc_Diszkret/MSc_kombi13/main.htm.

[5] Hajnal Péter: Algoritmusok és bonyolultságelmélet, 2015.
URL http://www.math.u-szeged.hu/~hajnal/courses/MSc_Bonyolultsag/main.htm.

[6] Morris W. Hirsch – Stephen Smale – Robert L. Devaney: *Differential Equations, Dynamical Systems and an Introduction to Chaos*. San Diego, 2004, Elsevier.

[7] Makay Géza: Jegyzet a dinamikus rendszerek c. tárgyhoz. Jegyzet, SZTE, Bolyai Intézet.

[8] Móricz Ferenc: *Numerikus módszerek az algebrában és az analízisben*. Szeged, 1997, Polygon.

[9] Móricz Ferenc: *Bevezetés a numerikus matematikába*. Szeged, 2008, Polygon.

[10] Németh Zoltán – Szabó Tamás: Jegyzet az alkalmazott analízis c. tárgyhoz. Jegyzet, 2013, SZTE, Bolyai Intézet.

[11] Pap Gyula – Szűcs Gábor: Sztochasztikus folyamatok. Jegyzet, 2014, SZTE, Bolyai Intézet, Sztochasztika Tanszék.

[12] Luis A. Santaló: *Integral Geometry and Geometric Probability*. Reading, 1976, Addison-Wesley.

[13] Skublics Benedek: Algoritmuselmélet – jegyzet Zádori László előadásához. Jegyzet, 2011, SZTE, Bolyai Intézet.

[14] George B. Thomas, Jr.: *Thomas-féle kalkulus – III. kötet*. Budapest, 2007, Typotex.