Robusne metode optimizacije u strojnom učenju

Čuklić, Martina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Martina Čuklić

ROBUSNE METODE OPTIMIZACIJE U STROJNOM UČENJU

Diplomski rad

Voditelj rada:
izv. prof. dr. sc.
Marko Vrdoljak

Zagreb, ožujak, 2023.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Strojno učenje područje je istraživanja posvećeno razumijevanju i izgradnji metoda koje 'uče', odnosno metoda koje koriste podatke za poboljšanje performansi na nekom skupu zadataka. Smatra se dijelom umjetne inteligencije. Brzo se razvija što je dovelo do mnogih teorijskih otkrića te se primjenjuje u raznim područjima. Optimizacija, kao važan dio strojnog učenja, privukla je veliku pažnju istraživača. S eksponencijalnim rastom količine podataka i povećanjem složenosti modela, metode optimizacije u strojnom učenju susreću se sa sve više i više izazova. Zato se puno radi na rješavanju problema optimizacije te unaprijeđenju metoda optimizacije u strojnom učenju. Od velike su važnosti sustavna retrospektiva i sažetak optimizacijskih metoda iz perspektive strojnog učenja, što može ponuditi smjernice za razvoj optimizacije te za istraživanje strojnog učenja.

Upravo učenje, optimizacija i donošenje odluka na temelju podataka često se moraju nositi s nesigurnosti. Nesigurnost može biti prisutna u podacima kada su izloženi smetnjama, kada nedostaju pretpostavke ili su neki čimbenici zanemareni. Čak i male nesigurnosti mogu imati veliki utjecaj na dopustivost rješenja. U strojnom učenju prenaučenost je središnji izazov te je za rješavanje tog problema razvijeno mnoštvo tehnika od kojih se mnoge temelje na regularizaciji.

Ovaj diplomski rad promatra i nesigurnost u optimizaciji i prenaučenost iz zajedničke perspektive - robusne optimizacije. Ona uvodi nove tehnike za dizajn algoritama koji su imuni na smetnje i savladavaju probleme prenaučenosti. Rad je organiziran na sljedeći način. U prvom poglavlju dan je kratki pregled robusne optimizacije i uvedeni su strojevi potpornih vektora. Mnogi postojeći algoritmi strojnog učenja koji se temelje na regularizaciji posebni su slučajevi robusne optimizacije pa je to najprije pokazano za strojeve potpornih vektora u prvom poglavlju, a u drugom za Lasso, ℓ_1 regulariziranu regresiju nakon što je definirana regularizacija. Robusnost je jako svojstvo koje se samo po sebi može koristiti kao put za istraživanje različitih svojstava rješenja. Tako je u drugom poglavlju pokazano da se robusnost može izravno koristiti za dokazivanje svojstava kao što su rijetkost, što je izuzetno važno svojstvo budući da poboljšava performanse modela, konzistentnost, koja osigurava da će procjene postati točnije kako se veličina uzorka povećava, te stabilnost. Ukratko, pokazano je da robusna optimizacija ima duboku vezu sa strojnim učenjem.

Poglavlje 1

Robusnost i stroj potpornih vektora

1.1 Robusna optimizacija

Optimizacija se koristi kako bi se našla najbolja rješenja problema gdje je "najbolje" obično definirano u terminima neke ciljne funkcije koja se treba minimizirati ili maksimizirati. Optimizacijski problemi mogu se naći u mnogim područjima. Neki primjeri su u ekonomiji kada treba odrediti optimalnu strategiju ulaganja, zatim u podatkovnom inženjerstvu gdje se moraju pronaći optimalni parametri za model strojnog učenja i tako dalje. Postoje različiti tipovi optimizacijskih problema, ali svima je zajedničko nalaženje vrijednosti jedne ili više varijabli koje će maksimizirati ili minimizirati ciljnu funkciju. Primjerice, u linearnom programiranju cilj je maksimizirati ili minimizirati linearnu funkciju uz linearna ograničenja.

Optimizacijom modeliramo kompliciranе probleme donošenja odluka u stvarnom svijetu. To nam često omogućava da dobijemo optimalna ili gotovo optimalna rješenja poprilično brzo. Dakle, modeliramo naše odluke koristeći varijable odluke, modeliramo našu ciljnu funkciju te obično imamo neka ograničenja, odnosno uvjete koji nam govore da nisu sve odluke dopustive. Međutim, često su i ciljna funkcija i uvjeti parametrizirani. To su parametri problema. Ako znamo parametre problema, taj problem je dobro definiran. No, u stvarnom svijetu obično ima puno nesigurnosti i zato se koriste parametri. Općenito:

$$\begin{array}{ll} \min_x & f(x, \xi) \\ \text{uz uvjete} & g(x, \xi) \leq 0. \end{array}$$

Ovdje su $\boldsymbol{x}$ varijable odluke, a $\boldsymbol{\xi}$ označava parametre problema.

Na početku su nam dani podaci i neki problem donošenja odluka. Na osnovu njih želimo izgraditi model za koji mislimo da dobro reprezentira problem koji želimo riješiti. Želimo dobiti točku (x, ξ) koja je dopustiva (zadovoljava sve uvjete) te optimalna ili gotovo optimalna. No, što s nesigurnosti? Uobičajeno, koristile bi se vjerojatnosne distribucije

kako bi se modelirala nesigurnost u podacima. Tada se radi o stohastičkom programiranju. Uzeli bismo podatke, dodijelili distribuciju i onda koristili distribuciju u našem problemu optimizacije. Međutim, teorija vjerojatnosti nije izgrađena s idejom da se koristi u problemima optimizacije. Namjera nije bila da imamo model koji nam samo omogućava da optimizacijske probleme riješimo brzo. Važno je da se problemi mogu riješiti brzo i jednostavno. U slučajevima kada imamo puno parametara nesigurnosti koji su jako povezani, kada ubacimo distribuciju u optimizacijski problem, dobijemo model koji ne možemo riješiti u razumnom vremenu. S druge strane, znamo efikasno riješiti probleme linearnog programiranja i općenitije, konveksne.

U robusnoj optimizaciji imamo deterministič an pogled na nesigurnost. Sama riječ robusnost označava otpornost na nesigurnost. Robusna optimizacija odmiče se od vjerojatnosnih distribucija, ali može koristiti teoriju vjerojatnosti da nas vodi u izgradnji modela, no ne koristi distribucije eksplicitno u modelu. Ideja robusne optimizacije je izgrađena na pretpostavci da parametri variraju proizvoljno unutar nekog unaprijed znanog ograničenog skupa - skupa nesigurnosti. Pretpostavimo da optimiziramo funkciju $f_0(x)$ s ograničenjima $f_i(x, u_i) \leq 0, i = 1, ..., m$ gdje je u_i parametar i-te funkcije. Dakle, gdje klasična optimizacija rješava $min_x\{f_o(x) : f_i(x, u_i) \leq 0, i = 1, ..., m\}$ uz pretpostavku da su u_i poznati, robusna optimizacija rješava:

$$\begin{array}{lll} min_x & : & f_0(x) \\ \text{uz uvjet} & : & f_i(x, u_i) \leq 0, u_i \in \mathcal{U}_i, i = 1, ..., m. \end{array} \tag{1.1}$$

Ovdje je $x \in \mathbb{R}^n$ vektor varijabli odluka, $f_0 : \mathbb{R}^n \to \mathbb{R}, f_i : \mathbb{R}^{n+k} \to \mathbb{R}$ su funkcije te su $u_i \in \mathbb{R}^k$ parametri nesigurnosti za koje pretpostavljamo da mogu poprimiti proizvoljne vrijednosti u skupu nesigurnosti $\mathcal{U}_i \subseteq \mathbb{R}^k$ za koji pretpostavljamo da je zatvoren. Cilj (1.1) je izračunati dopustivu točku x^* tako da su "troškovi" minimalni među svim rješenjima koja jesu dopustiva za sve realizacije u_i unutar $\mathcal{U}_i$. Ako neki $\mathcal{U}_i$ nisu diskretni skupovi, jasno je da problem (1.1) ima beskonačan broj uvjeta. Stoga sam zadatak pronalaska dopustive točke djeluje zahtjevan.

Nije skroz jasno kada je (1.1) efikasno rješiv. Moglo bi se pomisliti da dodavanje robusnosti generalnom problemu optimizacije dolazi po cijeni povećane računalne složenosti. Ispostavlja se da je to istina te je robusna inačica proizvoljnom problemu konveksne optimizacije zahtjevna. Unatoč tome, postoje mnogi robusni problemi koji mogu biti nezahtjevni i mnogo je literature fokusirano na specifikaciju klasa funkcija f_i, zajedno s tipovima skupova nesigurnosti $\mathcal{U}_i$, koje nam daju izvedive robusne inačice.

U ovom odjeljku opisujemo nekoliko strukturnih svojstava i opisujemo neke rezultate zahtjevnosti dobivanja rješenja zadaće robusne optimizacije (detalji se mogu naći u [2] i [5]).

Definirajmo robusni dopustivi skup na sljedeći način

$$X(\mathcal{U}) = \{\boldsymbol{x} \in \mathbb{R}^n : f_i(\boldsymbol{x}, \boldsymbol{u}_i) \leq 0, \boldsymbol{u}_i \in \mathcal{U}_i, i = 1, \ldots, m\}. \tag{1.2}$$

Pokazuje se da je problem efikasno rješiv uz pretpostavku konveksnosti od $X(\mathcal{U})$ s efikasnim testom separacije.
Robusna inačica zadaće linearnog programiranja, bez smanjenja općenitosti, izgleda ovako:

$$\begin{aligned} &\text{minimiziraj } \boldsymbol{c}^\top \boldsymbol{x} \\ &\text{uz uvjete } \boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{b} \quad \mathbf{a}_1 \in \mathcal{U}_1, \ldots, \mathbf{a}_m \in \mathcal{U}_m, \end{aligned} \tag{1.3}$$

gdje $\mathbf{a}_i$ predstavlja i-ti red matrice nesigurnosti A i poprima vrijednosti u skupu nesigurnosti $\mathcal{U}_i \subseteq \mathbb{R}^n$. Tada vrijedi $\boldsymbol{a}_i^\top \boldsymbol{x} \leq b_i$ za svaki $\boldsymbol{a}_i \in \mathcal{U}_i$ ako i samo ako $\max_{\{\boldsymbol{a}_i \in \mathcal{U}_i\}} \boldsymbol{a}_i^\top \boldsymbol{x} \leq b_i$ za svaki i. To je potproblem koji se mora riješiti. Robusna inačica zadaće linearnog programiranja je efikasno rješiva za većinu skupova nesigurnosti koji su od interesa. Doduše, tada rezultirajući problem ne mora više biti linearan.

Razmotrimo elipsoidne skupove nesigurnosti.

Teorem 1.1.1. *Neka je $\mathcal{U}$ elipsoidan, tj.*

$$\mathcal{U} = U(\Pi, Q) = \{\Pi(u) : \|Qu\| \leq \rho\}$$

gdje $\boldsymbol{u} \to \Pi(\boldsymbol{u})$ je afino ulaganje od $\mathbb{R}^L$ u $\mathbb{R}^{m \times n}$ i $Q \in \mathbb{R}^{M \times L}$. Tada je problem (1.3) *ekvivalentan problemu konusnog programiranja drugog reda. Eksplicitno, ako imamo*

$$\begin{aligned} &\textit{minimiziraj } \boldsymbol{c}^\top \boldsymbol{x} \\ &\textit{uz uvjete } \boldsymbol{a}_i \boldsymbol{x} \leq b_i \quad \forall \boldsymbol{a}_i \in \mathcal{U}_i \quad \forall i = 1, \ldots, m, \end{aligned}$$

gdje je skup nesigurnosti sljedeći

$$\mathcal{U} = \left\{(a_1, \ldots, a_m) : a_i = a_i^0 + \Delta_i u_i, i = 1, \ldots, m, \quad \|u\|_2 \leq \rho\right\}$$

tada je robusna inačica sljedeća

$$\begin{aligned} &\textit{minimiziraj } \boldsymbol{c}^\top \boldsymbol{x} \\ &\textit{uz uvjete } \boldsymbol{a}_i^0 \boldsymbol{x} \leq b_i - \rho \|\Delta_i \boldsymbol{x}\|_2 \quad \forall i = 1, \ldots, m \end{aligned}$$

Postoje dostupni alati za rješavanje problema konusnog programiranja drugog reda koji ga mogu efikasno riješiti.

Razmotrimo sada poliedarsku nesigurnost. Poliedarska nesigurnost može se promatrati kao poseban slučaj elipsoidne nesigurnosti. Kada je $\mathcal{U}$ poliedarski skup, potproblem postaje linearan i robusna inačica je zadaća linearnog programiranja. Kako bismo to ilustrirali, promotrimo sljedeći problem

$$\begin{aligned} &\text{minimiziraj } \boldsymbol{c}^\top \boldsymbol{x} \\ &\quad \text{uz uvjete } \max_{\{\boldsymbol{D}_i \boldsymbol{a}_i \leq \boldsymbol{d}_i\}} \boldsymbol{a}_i^\top \boldsymbol{x} \leq b_i, \quad i = 1, \ldots, m. \end{aligned}$$

Dual potproblema postaje

$$\left[\begin{array}{ll} \text{maksimiziraj} & \boldsymbol{a}_i^\top \boldsymbol{x} \\ \text{uz uvjete} & \boldsymbol{D}_i \boldsymbol{a}_i \leq \boldsymbol{d}_i \end{array}\right] \longleftrightarrow \left[\begin{array}{ll} \text{minimiziraj} & \boldsymbol{p}_i^\top \boldsymbol{d}_i \\ \text{uz uvjete} & \boldsymbol{p}_i^\top \boldsymbol{D}_i = \boldsymbol{x}^T \\ & \boldsymbol{p}_i \geq 0 \end{array}\right]$$

te zato robusno linearno programiranje postaje

$$\begin{aligned} &\text{minimiziraj } \boldsymbol{c}^\top \boldsymbol{x} \\ &\quad \text{uz uvjete } \boldsymbol{p}_i^\top \boldsymbol{d}_i \leq b_i, \quad i = 1, \ldots, m, \\ &\qquad\qquad \boldsymbol{p}_i^\top \boldsymbol{D}_i = \boldsymbol{x}, \quad i = 1, \ldots, m, \\ &\qquad\qquad \boldsymbol{p}_i \geq 0, \quad i = 1, \ldots, m. \end{aligned}$$

Složenost takvog problema raste polinomno sa složenošću nominalnog problema i dimenzijom skupa nesigurnosti.

Razmatramo sljedeći oblik nesigurnosti. Neka je matrica nesigurnosti $\boldsymbol{A} = \left(a_{ij}\right)$ takva da svaki element a_{ij} leži u $\left[a_{ij} - \hat{a}_{ij}, a_{ij} + \hat{a}_{ij}\right]$. Dopuštamo da najviše Γ_i elemenata i-tog retka odstupa. S danim vrijednostima $\Gamma_1, \ldots, \Gamma_m$ robusna formulacija postaje

$$\begin{array}{lll} \text{minimiziraj} & \boldsymbol{c}^\top \boldsymbol{x} & \\ \text{uz uvjete} & \sum_j a_{ij} x_j + \max_{\{S_i \subseteq J_i : |S_i| = \Gamma_i\}} \sum_{j \in S_i} \hat{a}_{ij} y_j \leq b_i, & 1 \leq i \leq m \\ & -y_j \leq x_j \leq y_j, & 1 \leq j \leq n \\ & l \leq \boldsymbol{x} \leq \boldsymbol{u} & \\ & \boldsymbol{y} \geq \boldsymbol{0}. & \end{array}$$

Zbog izbora skupa u unutarnjoj maksimizaciji, problem nije konveksan. No, ako relaksiramo problem konveksifikacijom i uzmemo dual unutarnjeg maksimizacijskog problema, pokaže se da je problem ekvivalentan sljedećoj linearnoj formulaciji, a time i efikasno rješiv.

$$\begin{array}{lll} \text{maksimiziraj} & \boldsymbol{c}^\top \boldsymbol{x} & \\ \text{uz uvjete} & \sum_j a_{ij} x_j + z_i \Gamma_i + \sum_j p_{ij} \leq b_i & , i, \\ & z_i + p_{ij} \geq \hat{a}_{ij} y_j & , i, j, \\ & -y_j \leq x_j \leq y_j & , j, \\ & l \leq \boldsymbol{x} \leq \boldsymbol{u}, & \\ & \boldsymbol{p} \geq \boldsymbol{0} & \\ & \boldsymbol{y} \geq \boldsymbol{0}. & \end{array}$$

Sljedeći teorem nam pokazuje da problemi robusne linearne optimizacije sa skupovima nesigurnosti koji su opisani općenitim normama su ekvivalentni konveksnom problemu s ograničenjima povezanim s dualnom normom. Oznaka vec($\boldsymbol{A}$) označava vektor koji je dobiven konkatenacijom svih redaka matrice A.
Prije teorema imamo jednu definiciju.

Definicija 1.1.2. *Ako je* $\|\cdot\|$ *norma, dualnu normu* $\|\cdot\|^*$ *definiramo s* $\|z\|^* = \sup\{z^\top x : \|x\| \leq 1\}$ *za proizvoljni z.*

Teorem 1.1.3. *Sa skupom nesigurnosti*

$$\mathcal{U} = \{\boldsymbol{A} : \|M(\mathrm{vec}(\boldsymbol{A}) - \mathrm{vec}(\overline{\boldsymbol{A}}))\| \leq \Delta\}, \tag{1.4}$$

gdje su M i $\bar{A}$ *zadane matrice, a M je invertibilna matrica i* $\|\cdot\|$ *je bilo koja norma, problem* (1.3) *je ekvivalentan sljedećem problemu*

$$\begin{array}{ll} \text{minimiziraj} & c^\top x \\ \textit{uz uvjete} & \overline{\boldsymbol{A}}_i^\top x + \Delta \left\| (M^\top)^{-1} x_i \right\|^* \leq b_i, \quad i = 1, \ldots, m, \end{array}$$

gdje je $\boldsymbol{x}_i \in \mathbb{R}^{(m\cdot n)\times 1}$ *vektor koji sadrži* $\boldsymbol{x} \in \mathbb{R}^n$ *na mjestima od* $(i-1)\cdot n + 1$ *do* $i \cdot n$ *i* 0 *na svim ostalim mjestima i* $\|\cdot\|^*$ *je dualna norma od* $\|\cdot\|$.

1.2 Stroj potpornih vektora s tvrdom i mekom marginom

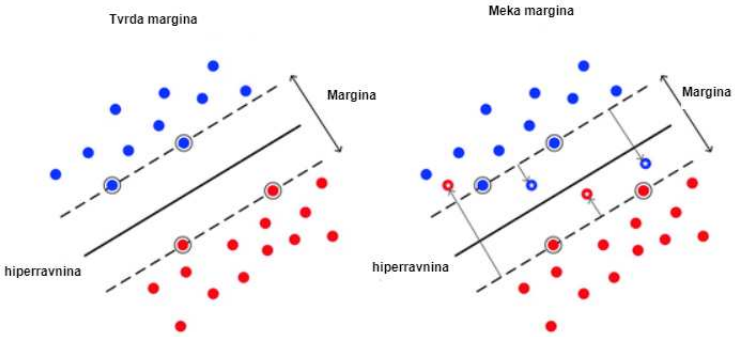
Algoritam stroja potpornih vektora (engl. *support vector machine*) rješava probleme klasifikacije, ali se također može koristiti u problemima regresije. Ideja je između svih hiperravnina odabrati upravo onu za koju je udaljenost do najbližeg primjera sa svake strane maksimalna (tu udaljenost zovemo marginom). Uzmimo skup parova za učenje (x_i, y_i) i = 1, . . . , m gdje su oznake y_i iz skupa $\{-1, +1\}$, a $x_i \epsilon \mathbb{R}^n$.

Podaci koje želimo odvojiti u dvije grupe mogu, ali i ne moraju biti linearno odvojivi. U slučaju kada podaci jesu linearno odvojivi i kada ne želimo dopustiti pogrešnu klasifikaciju, koristimo stroj potpornih vektora s tvrdom marginom. No, kada linearna granica nije izvediva, možemo dozvoliti neke pogrešne klasifikacije i odabrati strojeve potpornih vektora s mekom marginom. Margina je udaljenost od hiperravnine do najbližih podataka i stroj potpornih vektora maksimizira marginu oko hiperravnine.

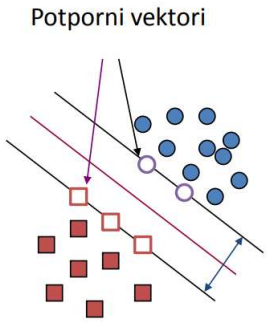
Primjerci koji su najbliži hiperravnini su potporni vektori. Možemo definirati marginu s dvije paralelne hiperravnine:

$$w^T x + \alpha = 0$$
$$w^T x + \beta = 0.$$

Uzmimo da ne dozvoljavamo pogrešne klasifikacije i želimo maksimizirati udaljenost između te dvije hiperravnine. Kako bismo našli tu udaljenost, koristimo formulu udaljenosti točke od ravnine. Imamo dvije udaljenosti, hiperravnine od potpornih vektora jedne klase i hiperravnine od potpornih vektora druge klase. Točnije:



Slika 1.1: Prikaz tvrde i meke margine



Slika 1.2: Prikaz potpornih vektora

$$\frac{|w^T x + \alpha|}{||w||}, \frac{|w^T x + \beta|}{||w||}.$$

Konačno, totalna margina je:

$$\frac{|\alpha - \beta|}{||w||}.$$

Tu marginu želimo maksimizirati. Bez smanjenja općenitosti možemo uzeti $\alpha = b + 1$ i $\beta = b - 1$. Iz toga slijedi da trebamo maksimizirati $\frac{2}{||w||}$, to jest minimizirati $\frac{||w||}{2}$. Koristit ćemo kvadriranu formu pa imamo:

$$\min_{w,b} \frac{1}{2}||w||^2 \equiv \min_{w,b} \frac{1}{2} w^T w.$$

Još preostaje zapisati uvjete. Budući da nam je skup oznaka {-1, +1}, mora vrijediti za primjerke koji ne pripadaju klasi da je $w^T x + b \leq -1$, a za primjerke koji pripadaju klasi $w^T x + b \geq 1$. Ta dva ograničenja možemo kombinirati u jedno:

$$y_i(w^T x_i + b) \geq 1.$$

Dakle, imamo optimizacijski problem:

$$\begin{aligned} \min \quad & \frac{1}{2} w^T w \\ & y_i(w^T x_i + b) \geq 1 \ , i = 1, \ldots, m. \end{aligned} \tag{1.5}$$

Stroj potpornih vektora s mekom marginom ima sličan optimizacijski problem, uz par manjih razlika. Budući da dozvoljavamo pogrešne klasifikacije, trebamo minimizirati grešku tih pogrešnih klasifikacija. To znači da moramo uvesti još jedno ograničenje. Trebamo uvesti i funkciju gubitka (kaznenu funkciju) koja se u ovom slučaju zove gubitak zglobnice (engl. *hinge loss*).

$$\max\{0, 1 - y_i(w^T x + b)\}.$$

Kažnjavanje tih pogrešno klasificiranih varijabli ćemo ostvariti uvođenjem pomoćnih varijabli, $\xi_i \geq 0$. Sada nam optimizacijski problem izgleda ovako:

$$\begin{aligned} \min_{\mathbf{w},b,\xi} : \quad & \frac{1}{2}\|w\|^2 + C \sum_{i=1}^{m} \xi_i \\ \text{uz uvjete} : \quad & \xi_i \geq \left[1 - y_i \left(\langle \mathbf{w}, \mathbf{x}_i \rangle + b\right)\right] \\ & \xi_i \geq 0. \end{aligned} \tag{1.6}$$

Parametar $C > 0$ određuje kompromis izmedu veličine margine i ukupne kazne. Veći C dovodi do većeg kažnjavanja pogrešne klasifikacije, što će za posljedicu imati složenije modele.

1.3 Robusnost i regularizacija

Sada razmatramo regularizirane strojeve potpornih vektora i pokazujemo da su algebarski ekvivalentni problemu robusne optimizacije [1]. Dakle, imamo skup za učenje $\{\mathbf{x}_i, y_i\}_{i=1}^m \subseteq \mathbb{R}^n \times \{-1, +1\}$ te je potrebno naći linearni klasifikator definiran kao $h^{\mathbf{w},b}(\mathbf{x}) = \text{sgn}(\mathbf{w}^T\mathbf{x} + b)$, a $r(\mathbf{w}, b)$ je regularizacijski član. Optimizacijski problem (1.6) sada zapišemo ovako

$$\begin{aligned} \min_{\mathbf{w},b,\xi} : \quad & r(\mathbf{w}, b) + \sum_{i=1}^{m} \xi_i \\ \text{s.t.} : \quad & \xi_i \geq \left[1 - y_i \left(\langle \mathbf{w}, \mathbf{x}_i \rangle + b\right)\right] \\ & \xi_i \geq 0. \end{aligned}$$

To je ekvivalentno sljedećem izrazu

$$\min_{\mathbf{w},b} \left\{ r(\mathbf{w}, b) + \sum_{i=1}^{m} \max\left[1 - y_i \left(\langle \mathbf{w}, \mathbf{x}_i \rangle + b\right), 0\right] \right\}.$$

Neka su značajke podložne poremećajima. Ovdje poremećaje označimo s $\mathbf{u} = (u_1, \ldots, u_m)$. Razmatramo aditivan model $\mathbf{x}_i - u_i$. Sada imamo sljedeći zapis

$$\min_{\mathbf{w},b} \max_{u \in \mathcal{U}} \left\{ r(\mathbf{w}, b) + \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \mathbf{w}, \mathbf{x}_i - u_i \rangle + b\right), 0\right] \right\},$$

gdje nam je $\mathcal{U}$ skup nesigurnosti. Kako bismo ga opisali, potrebno nam je još nekoliko definicija.

Definicija 1.3.1. *Skup $\mathcal{U}_0 \subseteq \mathbb{R}^n$ zovemo atomarnim skupom nesigurnosti ako vrijedi*

1. $0 \in \mathcal{U}_0$;
2. *za svaki* $\mathbf{w}_0 \in \mathbb{R}^n$ *vrijedi* $\sup_{u \in \mathcal{U}_0} \left[\mathbf{w}_0^\top \boldsymbol{u}\right] = \sup_{u' \in \mathcal{U}_0} \left[-\mathbf{w}_0^\top \boldsymbol{u}'\right] < +\infty$.

Drugi uvjet nam zapravo govori da je skup nesigurnosti ograničen i simetričan u smislu da su mu potporne hiperravnine centralnosimetrične s obzirom na ishodište.

Definicija 1.3.2. *Neka je $\mathcal{U}_0$ atomarni skup nesigurnosti. Skup $\mathcal{U} \subseteq \mathbb{R}^{n \times m}$ zovemo sublinearnim agregiranim skupom nesigurnosti od $\mathcal{U}_0$ ako*

$$\mathcal{U}^- \subseteq \mathcal{U} \subseteq \mathcal{U}^+,$$

gdje

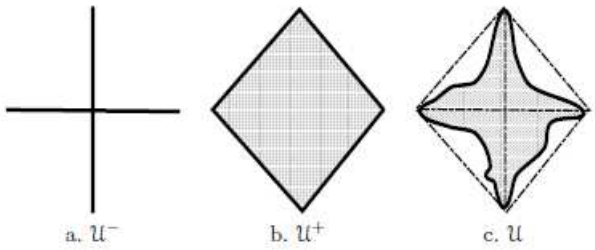
$$\mathcal{U}^- := \bigcup_{t=1}^{m} \mathcal{U}_t^-; \quad \mathcal{U}_t^- := \{(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) : \boldsymbol{u}_t \in \mathcal{U}_0; \boldsymbol{u}_i = \mathbf{0}, i \neq t\}$$

$$\mathcal{U}^+ := \left\{(\alpha_1 \boldsymbol{u}_1, \ldots, \alpha_m \boldsymbol{u}_m) : \sum_{} \alpha_i = 1; \alpha_i \geq 0, \boldsymbol{u}_i \in \mathcal{U}_0, i = 1, \ldots, m\right\}.$$

Sublinearna agregirana nesigurnost modelira slučaj u kojem se poremećaji na svakom uzorku tretiraju identično, ali se kontrolira njihovo zajedničko ponašanje na više uzoraka. Neki od zanimljivih primjera su

1. $\mathcal{U} = \{(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) : \sum^m \|\boldsymbol{u}_i\| \leq c\}$
2. $\mathcal{U} = \{(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) : \exists t \in [1, \ldots, m]; \|\boldsymbol{u}_t\| \leq c; \boldsymbol{u}_i = \mathbf{0}, \forall i \neq t\}$
3. $\mathcal{U} = \left\{(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m) : \sum_{i=1}^m \sqrt{\|\boldsymbol{u}_i\|} \leq \frac{c}{\sqrt{c}}\right\}$

Svi ti primjeri dijele isti atomarni skup nesigurnosti $\mathcal{U}_0 = \{\boldsymbol{u} \mid \|\boldsymbol{u}\| \leq c\}$. Sljedeći teorem je glavni rezultat ovog poglavlja koji dokazuje da je standardni regularizirani stroj potpornih vektora rješenje (neregularizirane) robusne optimizacije.



Slika 1.3: Sublinearni agregirani skup nesigurnosti $\mathcal{U}$

Teorem 1.3.3. *Neka* $\{\mathbf{x}_i, y_i\}_{i=1}^m$ *nije linearno odvojiv,* $r(\cdot,\cdot) : \mathbb{R}^{n+1} \to \mathbb{R}$ *je proizvoljna funkcija i* $\mathcal{U}$ *je sublinearni agregirani skup nesigurnosti s pripadajućim atomarnim skupom nesigurnosti* $\mathcal{U}_0$*. Tada je sljedeći min-max problem*

$$\min_{\mathbf{w},b} \sup_{(\mathbf{u}_1,\ldots,\mathbf{u}_m)\in\mathcal{U}} \left\{ r(\mathbf{w},b) + \sum_{i=1}^{m} \max \mid \left[1 - y_i\left(\langle \mathbf{w}, \mathbf{x}_i - \boldsymbol{u}_i\rangle + b\right), 0\right] \right\} \tag{1.7}$$

ekvivalentan sljedećem problemu optimizacije

$$\begin{gathered} \min_{\mathbf{w},b,\boldsymbol{\xi}} : r(\mathbf{w},b) + \sup_{\boldsymbol{u}\in\mathcal{U}_0} \left(\mathbf{w}^\top \boldsymbol{u}\right) + \sum_{i=1}^{m} \xi_i \\ \textit{uz uvjete} : \xi_i \geq 1 - \left[y_i\left(\langle \mathbf{w}, \mathbf{x}_i\rangle + b\right)\right], \quad i = 1,\ldots,m \\ \xi_i \geq 0, \quad i = 1,\ldots,m. \end{gathered} \tag{1.8}$$

Nadalje, problem (1.8) *ima rješenje kada je r odozdo poluneprekidna.*

Dokaz. Definirajmo:

$$v(\mathbf{w},b) := \sup_{u\in\mathcal{U}_0} \left(\mathbf{w}^\top u\right) + \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \mathbf{w}, \mathbf{x}_i\rangle + b\right), 0\right].$$

Sjetimo se da je po definiciji $\mathcal{U}^- \subseteq \mathcal{U} \subseteq \mathcal{U}^+$. Kad fiksiramo $(\hat{\mathbf{w}}, \hat{b}) \in \mathbb{R}^{n+1}$, vrijede sljedeće nejednakosti:

$$\begin{aligned} &\sup_{(\mathbf{u}_1,\cdots,\mathbf{u}_m)\in\mathcal{U}^-} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \mathbf{u}_i\rangle + \hat{b}\right), 0\right] \\ \leq &\sup_{(\mathbf{u}_1,\cdots,\mathbf{u}_m)\in\mathcal{U}} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \mathbf{u}_i\rangle + \hat{b}\right), 0\right] \\ \leq &\sup_{(\mathbf{u}_1,\cdots,\mathbf{u}_m)\in\mathcal{U}^+} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \mathbf{u}_i\rangle + \hat{b}\right), 0\right]. \end{aligned}$$

Kako bismo dokazali teorem, najprije pokazujemo da $v(\hat{\mathbf{w}}, \hat{b})$ nije veći od prvog od gornja tri supremuma, a zatim pokazujemo da $v(\hat{\mathbf{w}}, \hat{b})$ nije manji od zadnjeg supremuma.
Prvi korak: Dokazujemo da

$$v(\hat{\mathbf{w}}, \hat{b}) \leq \sup_{(\mathbf{u}_1, \cdots, \mathbf{u}_m) \in \mathcal{U}^-} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \mathbf{u}_i \rangle + \hat{b}\right), 0\right]. \tag{1.9}$$

Obzirom da uzorci $\{\mathbf{x}_i, y_i\}_{i=1}^m$ nisu odvojivi, postoji $t \in \{1, \ldots, m\}$ takav da

$$y_t\left(\langle \hat{\mathbf{w}}, \mathbf{x}_t \rangle + \hat{b}\right) < 0. \tag{1.10}$$

Zato,

$$\begin{aligned}
&\sup_{(\mathbf{u}_1, \cdots, \mathbf{u}_m) \in \mathcal{U}_t^-} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \mathbf{u}_i \rangle + \hat{b}\right), 0\right] \\
&= \sum_{i \neq t} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i \rangle + \hat{b}\right), 0\right] + \sup_{\mathbf{u}_t \in \mathcal{U}_0} \max\left[1 - y_t\left(\langle \hat{\mathbf{w}}, \mathbf{x}_t - \mathbf{u}_t \rangle + \hat{b}\right), 0\right] \\
&= \sum_{i \neq t} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i \rangle + \hat{b}\right), 0\right] + \max\left[1 - y_t\left(\langle \hat{\mathbf{w}}, \mathbf{x}_t \rangle + \hat{b}\right) + \sup_{\mathbf{u}_t \in \mathcal{U}_0} \left(y_t \hat{\mathbf{w}}^\top \mathbf{u}_t\right), 0\right] \\
&= \sum_{i \neq t} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i \rangle + \hat{b}\right), 0\right] + \max\left[1 - y_t\left(\langle \hat{\mathbf{w}}, \mathbf{x}_t \rangle + \hat{b}\right), 0\right] + \sup_{\mathbf{u}_t \in \mathcal{U}_0} \left(y_t \hat{\mathbf{w}}^\top \mathbf{u}_t\right) \\
&= \sup_{u \in \mathcal{U}_0} (\hat{\mathbf{w}}^\top \mathbf{u}) + \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i \rangle + \hat{b}\right), 0\right] = v(\hat{\mathbf{w}}, \hat{b}).
\end{aligned}$$

Treća jednakost vrijedi zbog nejednakosti (1.10) i zato što je $\sup_{u_t \in \mathcal{U}_0} \left(y_t \hat{\mathbf{w}}^\top u_t\right)$ nenegativan ($\mathbf{0} \in \mathcal{U}_0$). Obzirom da je $\mathcal{U}_t^- \subseteq \mathcal{U}^-$, nejednakost (1.9) vrijedi.
Drugi korak: Sada dokazujemo da

$$\sup_{(\mathbf{u}_1, \cdots, \mathbf{u}_m) \in \mathcal{U}^+} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \mathbf{u}_i \rangle + \hat{b}\right), 0\right] \leq v(\hat{\mathbf{w}}, \hat{b}). \tag{1.11}$$

Primijetimo da po definiciji od $\mathcal{U}^+$ imamo

$$\begin{aligned}
&\sup_{(\mathbf{u}_1, \cdots, \mathbf{u}_m) \in \mathcal{U}^+} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \mathbf{u}_i \rangle + \hat{b}\right), 0\right] \\
&= \sup_{\sum_{i=1}^m \alpha_i = 1; \alpha_i \geq 0; \hat{\mathbf{u}}_i \in \mathcal{U}_0} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \alpha_i \hat{\mathbf{u}}_i \rangle + \hat{b}\right), 0\right] \qquad (1.12) \\
&= \sup_{\sum_{i=1}^m \alpha_i = 1; \alpha_i \geq 0} \sum_{i=1}^{m} \max\left[\sup_{\hat{\mathbf{u}}_i \in \mathcal{U}_0} \left(1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \alpha_i \hat{\mathbf{u}}_i \rangle + \hat{b}\right)\right), 0\right].
\end{aligned}$$

Za svaki $i \in \{1, \ldots, m\}$ vrijedi sljedeće

$$\begin{aligned}
&\max\left[\sup_{\hat{\mathbf{u}}_i \in \hat{\mathcal{U}}_0}\left(1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i - \alpha_i \hat{\mathbf{u}}_i\rangle + \hat{b}\right)\right), 0\right] \\
&= \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i\rangle + \hat{b}\right) + \alpha_i \sup_{\hat{\mathbf{u}}_i \in \mathcal{U}}\left(\hat{\mathbf{w}}^\top \hat{\mathbf{u}}_i\right), 0\right] \\
&\leq \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i\rangle + \hat{b}\right), 0\right] + \alpha_i \sup_{\hat{\mathbf{u}}_i \in \mathcal{U}0}\left(\hat{\mathbf{w}}^\top \hat{\mathbf{u}}_i\right).
\end{aligned}$$

Dakle, vrijednost (1.12) je odozgo ograničena s

$$\begin{aligned}
&\sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i\rangle + \hat{b}\right), 0\right] + \sup_{\sum_{i=1}^m \alpha_i = 1; \alpha_i \geq 0} \sum_{i=1}^{m} \alpha_i \sup_{\hat{\mathbf{u}}_i \in \mathcal{U}_0}\left(\hat{\mathbf{w}}^\top \hat{\mathbf{u}}_i\right) \\
&= \sup_{\mathbf{u} \in \mathcal{U}_0}\left(\hat{\mathbf{w}}^\top \mathbf{u}\right) + \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \hat{\mathbf{w}}, \mathbf{x}_i\rangle + \hat{b}\right), 0\right] = v(\hat{\mathbf{w}}, \hat{b})
\end{aligned}$$

pa (1.11) vrijedi.
Treći korak: Kombinirajući prethodna dva koraka i dodavanjem $r(\mathbf{w}, b)$ na obje strane vodi do toga da vrijedi za svaki $(\mathbf{w}, b) \in \mathbb{R}^{n+1}$

$$\sup_{(\mathbf{u}_1, \cdots, \mathbf{u}_m) \in \mathcal{U}} \sum_{i=1}^{m} \max\left[1 - y_i\left(\langle \mathbf{w}, \mathbf{x}_i - \mathbf{u}_i\rangle + b\right), 0\right] + r(\mathbf{w}, b) = v(\mathbf{w}, b) + r(\mathbf{w}, \mathbf{b}).$$

Kad uzmemo infinum na obje strane, dobivamo ekvivalenciju (1.7) i (1.8). Primijetimo da je $\sup_{\mathbf{u} \in \mathcal{U}_0} \mathbf{w}^\top \mathbf{u}$ supremum afinih funkcija i zato je odozdo poluneprekinut pa onda je i $\boldsymbol{\nu}$. Stoga se postiže minimum u problemu (1.8), ako je r odozdo poluneprekidna, a tada se, zbog ekvivalentnosti, postiže minimum u problemu (1.7).

□

Poglavlje 2

Robusnost u problemu regresije

2.1 Uvod

Kod nadziranog učenja imamo ulazne podatke tipa (x,y) pri čemu je $x = (x_1, x_2, ..., x_n)$ vektor značajki, a y ciljna vrijednost dane instance. Ulazne podatke nazivamo primjerima. S $\mathcal{D} = \left\{\left(\mathbf{x}^{(i)}, y^{(i)}\right)\right\}$ označavamo skup primjeraka za učenje. Cilj nadziranog učenja je pronaći preslikavanje koje nam za dane ulazne podatke daje ciljnu vrijednost y, tj. pronalazi funkciju f takvu da vrijedi $f(x) = y$. Postupcima nadziranog učenja mogu se rješavati dvije vrste problema: klasifikacija i regresija.
Kod klasifikacije primjeru pridružujemo klasu (razred) kojoj taj primjer pripada. Kod regresije primjeru pridružujemo neku kontinuiranu vrijednost. Dakle, razlika je u tome je li ciljna varijabla diskretna ili nominalna (klasifikacija) ili je kontinuirana (regresija).

Regresijom nad skupom za učenje $\mathcal{D}$ dobivamo funkciju, odnosno hipotezu h kao aproksimaciju funkcije f. Empirijska pogreška hipoteze h na $\mathcal{D}$ najjednostavnije se može definirati kao

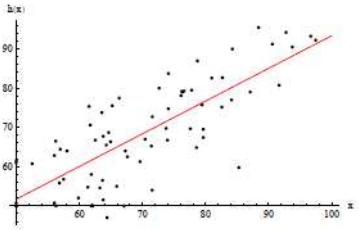
$$E(h \mid \mathcal{D}) = \frac{1}{2} \sum_{i=1}^{N} \left(y^{(i)} - h\left(\mathbf{x}^{(i)}\right)\right)^2 .$$

Vidimo da pogrešku prikazujemo kao zbroj kvadratnih vrijednosti odstupanja predviđene vrijednosti hipoteze $h(x)$ i ciljne vrijednosti y.
Promotrimo linearan model (želimo da minimizira empirijsku pogrešku). Dakle, imamo:

$$h(\mathbf{x}) = w_1 x_1 + w_2 x_2 + \cdots + w_n x_n + w_0 = \sum_{i=1}^{n} w_i x_i + w_0 = \mathrm{w}^{\mathrm{T}}\mathbf{x} + w_0.$$

Tu su w_i parametri koje treba naučiti na temelju skupa primjeraka $\mathcal{D}$. Još ih zovemo težinama. Ovu vrstu regresije onda nazivamo linearnom regresijom. Budući da je empirijska pogreška dana kao zbroj kvadrata pogrešaka koje nastaju na pojedinačnim primjerima,

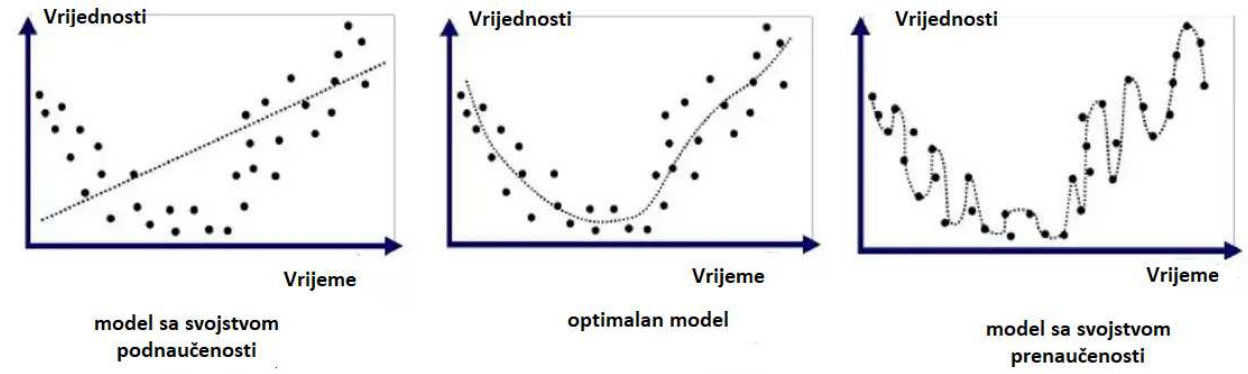
radi se o metodi najmanjih kvadrata. Kod regresije može doći do dva problema - pre-



Slika 2.1: Linearna regresija

naučenosti (engl. *overfitting*) i podnaučenosti (engl. *underfitting*). U slučaju da je model previše složen u odnosu na stvarnu funkciju, radi se o prenaučenosti. Model u tom slučaju preblizu ili točno odgovara određenom skupu podataka, može se prilagoditi svakom šumu u podacima te stoga neće moći pouzdano predvidjeti buduća opažanja.

Ako je model prejednostavan u odnosu na stvarnu funkciju, radi se o podnaučenosti. Hipoteza se ne može dovoljno prilagoditi stvarnim podacima, ne prepoznaje ključne značajke te takav model ima lošu prediktivnu izvedbu. Kako bi se spriječila prenaučenost, postoji



Slika 2.2: Podnaučenosti i prenaučenost

nekoliko mogućih mehanizama. Neki od njih su:

1. korištenje više primjera za učenje
2. odabir podskupa značajki modela

3. redukcija dimenzije
4. regularizacija
5. bayesovski odabir modela

Reći ćemo nešto više o regularizaciji koja je jedna osnovna, ali vrlo učinkovita i česta tehnika za spriječavanje prenaučenosti. Ona spaja učenje modela i postupak odabira modela na način da se u funkciju pogreške eksplicitno ugradi mjera složenosti modela. Tako se zapravo sprječava da model postane suviše složen jer će sa složenošću modela rasti njegova ukupna pogreška.

Sada općenito možemo zapisati regulariziranu funkciju pogreške na sljedeći način

$$E_R(\mathbf{w} \mid \mathcal{D}) = E(\mathbf{w} \mid \mathcal{D}) + \lambda\Omega(\mathbf{w}).$$

Ovdje je $E(\mathbf{w} \mid \mathcal{D})$ empirijska pogreška, a $\lambda\Omega(\boldsymbol{w})$ regularizacijski izraz gdje funkcija Ω karakterizira složenost modela, a λ je regularizacijski faktor. Svrha regularizacijskog faktora λ je da damo veći ili manji značaj jednoj ili drugoj komponenti. Primjerice, ako je $\lambda = 0$, imamo neregulariziranu funkciju pogreške. Što je λ veća, više se kažnjava složenost modela i u konačnici dobivamo jednostavnije modele.
Funkcija Ω ovisi o težinama $w_1, w_2, ..., w_n$. Kada su težine velike, želimo da je vrijednost od Ω velika, a mala kad su težine male. Možemo onda Ω promatrati kao p-normu vektora težina $\mathbf{w}$ koja je definirana na sljedeći način:

$$\|\mathbf{w}\|_p = \left(\sum_{j=1}^{n} \left| w_j \right|^p \right)^{\frac{1}{p}}.$$

Često p-norme označavamo s ℓ_p. Posebno, ℓ_1 norma je jednaka $\|\mathbf{w}\|_1 = \sum_{j=1}^{m} \left| w_j \right|$, a ℓ_2 norma $\|\mathbf{w}\|_2 = \sqrt{\sum_{j=1}^{m} w_j^2} = \sqrt{\mathbf{w}^\top \mathbf{w}}$. Kod korištenja ℓ_2 norme govorimo o ℓ_2 regularizirano regresiji, još zvanom i Tikhonovljeva ili hrbatna (engl. *ridge regression*), a u slučaju korištenja ℓ_1 regularizacije, govorimo o ℓ_1 regulariziranoj regresiji, tzv. Lasso (engl. *Least Absolute Shrinkage and Selection Operator*) regularizacija.
Empirijska pogreška kod ℓ_2 regularizirane regresije s pogreškom najmanjih kvadrata izgleda ovako:

$$E_R(\mathbf{w} \mid \mathcal{D}) = \frac{1}{2} \sum_{i=1}^{m} \left(\mathbf{w}^\top \phi\left(\mathbf{x}^i\right) - y^i \right)^2 + \frac{\lambda}{2} \|\mathbf{w}\|_2^2 l,$$

gdje je m broj značajki, a ϕ preslikava u prostor značajki.
Na sljedeći način definiramo empirijsku pogrešku kod ℓ_1 regularizirane regresije s pogreškom najmanjih kvadrata:

$$E(\mathbf{w} \mid \mathcal{D}) = \frac{1}{2} \sum_{i=1}^{m} \left(\mathbf{w}^\top \phi\left(\mathbf{x}^i\right) - y^i \right)^2 + \frac{\lambda}{2} \|\mathbf{w}\|_1.$$

Glavna razlika između tih regularizacija je upravo vidljiva kod malih težina koje su blizu nule, ℓ_1 regularizacija nema kvadrat pa će te težine kažnjavati više od ℓ_2 regularizacije. Zbog toga je za očekivati da će ℓ_1 regularizacija rezultirati modelima kod kojih je više težina postavljeno upravo na nulu, to jest rezultirat će rijeđim modelima.

Dobro je poznato da minimizacija pogreške najmanjih kvadrata može dovesti do rješenja koja su jako osjetljiva na male promjene danih podataka. Mnoge metode regularizacije su predlagane kako bi se smanjila ta osjetljivost. Jedne od njih su prethodno spomenute regularizacije - Tikhonovljeva i Lasso. Dodatno, Lasso je poznat zbog sklonosti da odabire rijetka rješenja.

Mnogi regularizirani problemi pokazuju "skrivenu robusnost", tj stabilnost kada su suočeni s nesigurnošću. Oni su zapravo ekvivalentni problemu robusne optimizacije—što se onda može koristiti za izravno dokazivanje svojstava kao što su konzistentnost i rijetkost, kao i za dizajn novih algoritama [4]. Tako je prvi rezultat ovog rada da rješenje Lasso regularizacije ima robusna svojstva, to jest rješenje je problema robusne optimizacije. Istražujemo problem robusne regresije gdje je skup nesigurnosti definiran ograničenjima koja se odnose na značajke. Takav model je od interesa kada se vrijednosti značajki dobiju s nekim šumom u koracima prethodne obrade, a veličine takvih šumova su poznate. Smetnje i skupovi nesigurnosti mogu biti ovisni i neovisni: intuitivno, govorimo o neovisnosti u kontekstu značajki ako nesigurnosti u različitim značajkama nisu povezane, a u suprotnom govorimo o ovisnosti.

Razmatranje rješenja Lasso regresije kao rješenja robusnog problema najmanjih kvadrata ima dvije važne posljedice. Prvo, robusnost osigurava vezu regularizatora s fizičkim svojstvom, naime, zaštitom od smetnji (šuma). To omogućuje odabir regularizatora na temelju svojstava smetnji. Štoviše, razmatranjem različitih skupova nesigurnosti, konstruiramo generalizacije Lasso regresije koje također daju probleme konveksne optimizacije.

Drugo, i možda najvažnije, robusnost je jako svojstvo koje se samo po sebi može koristiti kao put za istraživanje različitih svojstava rješenja. Pokazujemo da robusnost rješenja može objasniti zašto je rješenje rijetko. Analiza, kao i specifični rezultati koje dobivamo, razlikuju se od standardnih rezultata rijetkosti, pružajući drugačiju geometrijsku intuiciju i šire se izvan postavki najmanjih kvadrata. Rezultati rijetkosti dobiveni za Lasso u konačnici ovise o činjenici da uvođenje dodatnih značajki izaziva veću ℓ_1 kaznu od smanjenja pogreške najmanjih kvadrata. Nasuprot tome, mi iskorištavamo činjenicu da je robusno rješenje, po definiciji, optimalno rješenje u najgorem mogućem slučaju. Naši rezultati pokazuju da je koeficijent rješenja različit od nule ako je odgovarajuća značajka relevantna pod svim dopuštenim poremećajima. Osim rijetkosti, također izravno koristimo robusnost kako bismo dokazali konzistentnost Lasso regresije. U sljedećem odjeljku formuliramo problem robusne regresije sa skupom nesigurnosti gdje su poremećaji značajki nezavisni i pokazujemo da je ova formulacija ekvivalentna problemu najmanjih kvadrata s regularizacijskim članom težinske ℓ_1-norme. Stoga, nudimo tumačenje Lasso regulariza-

cije iz perspektive robusnosti.

Problem je naći vektor $\mathbf{x}$ tako da je ℓ_2 norma reziduala, odnosno odstupanja od predviđene vrijednosti, $\mathbf{b} - A\mathbf{x}$ minimizirana za danu matricu $\mathrm{A} \in \mathbb{R}^{n\times m}$ i vektor $\mathbf{b} \in \mathbb{R}^n$. Iz perspektive regresije, svaki redak od A promatramo kao uzorak za učenje, a odgovarajući element od $\mathbf{b}$ kao ciljnu vrijednost tog promatranog uzorka. Svaki stupac od A odgovara značajki, a cilj je naći skup težina tako da težinska suma vrijednosti značajki aproksimira ciljnu vrijednost. Što se tiče ostalih oznaka, $\mathbf{a}_i$ je i-ti stupac matrice A, a_{ij} je element na poziciji ij. Matrica ΔA predstavlja matricu poremećaja. Poremećaje značajki označavamo s δ_i, a to su vrijednosti unutar skupa nesigurnosti.

2.2 Regresija s poremećajima u značajkama

Regresijska formulacija koju razmatramo razlikuje se od standardne Lasso formulacije jer minimiziramo normu pogreške, a ne kvadrat norme. Može se pokazati da je ovo dvoje isto do na promjenu koeficijenta regularizacije, budući da je skup rješenja za bilo koju formulaciju Pareto učinkovit skup regresijske pogreške i kazne regularizacije.

Robusna linearna regresija razmatra slučaj kada je promatrana matrica oštećena nekim potencijalno zlonamjernim poremećajem. Cilj je pronaći optimalno rješenje u najgorem slučaju. Ovo se obično formulira kao sljedeći min-max problem,

$$\min_{\mathbf{x}\in\mathbb{R}^m} \left\{ \max_{\Delta A\in\mathcal{U}} \|\mathbf{b} - (A + \Delta A)\mathbf{x}\|_2 \right\}, \tag{2.1}$$

gdje se $\mathcal{U}$ naziva skup nesigurnosti ili skup dopuštenih poremećaja matrice A. U ovom odjeljku razmatramo klasu skupova nesigurnosti neovisnima o značajkama, to jest koji vežu normu poremećaja za svaku značajku, bez postavljanja ikakvih zajedničkih zahtjeva na poremećaje značajki. To jest, razmatramo klasu skupova nesigurnosti:

$$\mathcal{U} := \{(\delta_1, \cdots, \delta_m) : \|\delta_i\|_2 \leq c_i, \quad i = 1, \cdots, m\} \tag{2.2}$$

za dani $c_i \geq 0$. Ove skupove nazivamo nepovezanim u odnosu na značajke. U sljedećem teoremu pokazujemo da upravo ovi nepovezani skupovi nesigurnosti ograničeni normom dovode do lako rješivog problema optimizacije.

Teorem 2.2.1. *Problem robusne regresije* (2.1) *sa skupom nesigurnosti* (2.2) *je ekvivalentan sljedećem problemu ℓ_1 regularizirane regresije*

$$\min_{\mathbf{x}\in\mathbb{R}^m} \left\{ \|\mathbf{b} - A\mathbf{x}\|_2 + \sum_{i=1}^{m} c_i |x_i| \right\}. \tag{2.3}$$

Dokaz. Fiksirajmo $\mathbf{x}^*$. Dokazujemo da $\max_{\Delta A \in \mathcal{U}} \|\mathbf{b} - (A + \Delta A)\mathbf{x}^*\|_2 = \|\mathbf{b} - A\mathbf{x}^*\|_2 + \sum_{i=1}^m c_i \left|x_i^*\right|$. Lijeva strana može se zapisati kao

$$\begin{aligned}
&\max_{\Delta A \in \mathcal{U}} \|\mathbf{b} - (A + \Delta A)\mathbf{x}^*\|_2 \\
&= \max_{\|\boldsymbol{\delta}_i\|_2 \le c_i} \|\mathbf{b} - (A + (\boldsymbol{\delta}_1, \cdots, \boldsymbol{\delta}_m))\,\mathbf{x}^*\|_2 \\
&= \max_{\|\boldsymbol{\delta}_i\|_2 \le c_i} \left\|\mathbf{b} - A\mathbf{x}^* - \sum_{i=1}^m x_i^* \delta_i\right\|_2 \\
&\le \max_{\|\boldsymbol{\delta}_i\|_2 \le c_i} \|\mathbf{b} - A\mathbf{x}^*\|_2 + \sum_{i=1}^m \left\|x_i^* \delta_i\right\|_2 \\
&\le \|\mathbf{b} - A\mathbf{x}^*\|_2 + \sum_{i=1}^m \left|x_i^*\right| c_i.
\end{aligned} \tag{2.4}$$

Sada, neka je

$$\mathbf{u} \triangleq \begin{cases} \frac{\mathrm{b} - A\mathrm{x}^*}{\|\ \mathrm{b} - A\mathrm{x}^*\|_2} & A\mathrm{x}^* \neq \mathbf{b} \\ \text{bilo koji vektor s jediničnom } \ell_2 \text{ normom} & \text{inače} \end{cases} \tag{2.5}$$

i stavimo $\delta_i^* \triangleq -c_i \operatorname{sgn}\left(x_i^*\right)\mathbf{u}$.
Uočimo da je $\left\|\delta_i^*\right\|_2 \le c_i$, odnosno vrijedi $\Delta A^* \triangleq \left(\delta_1^*, \cdots, \delta_m^*\right) \in \mathcal{U}$. Uočimo sada da

$$\begin{aligned}
&\max_{\Delta A \in \mathcal{U}} \|\mathbf{b} - (A + \Delta A)\mathbf{x}^*\|_2 \\
&\ge \|\mathbf{b} - (A + \Delta A^*)\,\mathbf{x}^*\|_2 \\
&= \left\|\mathbf{b} - (A + (\delta_1^*, \cdots, \delta_m^*))\,\mathbf{x}^*\right\|_2 \\
&= \left\|(\mathbf{b} - A\mathbf{x}^*) - \sum_{i=1}^m \left(-x_i^* c_i \operatorname{sgn}\left(x_i^*\right)\mathbf{u}\right)\right\|_2 \\
&= \left\|(\mathbf{b} - A\mathbf{x}^*) + \left(\sum_{i=1}^m c_i \left|x_i^*\right|\right)\mathbf{u}\right\|_2 \\
&= \|\mathbf{b} - A\mathbf{x}^*\|_2 + \sum_{i=1}^m c_i \left|x_i^*\right|.
\end{aligned} \tag{2.6}$$

Zadnja jednadžba slijedi iz definicije od $\mathbf{u}$ budući da ima isti smjer i orijentaciju kao i $\mathbf{b} - A\mathbf{x}^*$.
Kombinirajući nejednakosti (2.4) i (2.6) dobivamo jednakost $\max_{\Delta A \in \mathcal{U}} \|\mathbf{b} - (A + \Delta A)\mathrm{x}^*\|_2 = \|\mathrm{b} - A\mathrm{x}^*\|_2 + \sum_{i=1}^m c_i \left|x_i^*\right|$ za svaki $\mathbf{x}^*$. Minimizacijom po $\mathbf{x}^*$ slijedi tvrdnja teorema. □

Kada stavimo $c_i = c$ i normiramo a_i za sve i, problem (2.3) nam predstavlja dobro znanu zadaću Lasso regresije.
U mnogim primjenama, šum δ_i je slučajan s poznatom distribucijom i moguće neograničenim vrijednostima koje može poprimiti. Stoga, robusna regresijska formulacija koja dopušta sve moguće ΔA može biti previše pesimistična ili čak besmislena. Jedan način za rješavanje tog problema je zamjena deterministčkog pristupa vjerojatnosnim, to jest pronaći parametar c_i takav da $\|\delta_i\|_2 \leq c_i$ vrijedi s danom pouzdanošću $1 - \eta$.

2.3 Skupovi nesigurnosti dani općom normom

Jedan od razloga zašto je robusna optimizacijska formulacija snažna je njezina fleksibilnost: nakon što smo pokazali vezu s ℓ_1 regulariziranom regresijom, Lassom, ona omogućuje generalizaciju na učinkovite algoritme za regularizaciju koji su "nalik na Lasso". U ovom odjeljku donosimo nekoliko generalizacija robusne formulacije (2.1) i izvodimo pandane Teoremu 2.2.1. Generaliziramo robusnu formulaciju na dva načina: (a) u slučaju proizvoljne norme; i (b) u slučaju skupova nesigurnosti gdje nesigurnosti u značajkama ovise međusobno. Prvo razmatramo slučaj proizvoljne norme $\|\ \|_a$ u $\mathbb{R}^n$ kao funkcije pogreške. Dokaz sljedećeg teorema je jednak dokazu Teorema 2.2.1, samo se radi o normi $\|\ \|_a$, a ne ℓ_2.

Teorem 2.3.1. *Problem robusne regresije*

$$\min_{\mathbf{x}\in\mathbb{R}^m}\left\{\max_{\Delta A\in\mathcal{U}_a}\|\mathbf{b}-(A+\Delta A)\mathbf{x}\|_a\right\};\quad \mathcal{U}_a \coloneqq \{(\delta_1,\cdots,\delta_m) : \|\boldsymbol{\delta}_i\|_a \leq c_i,\quad i=1,\cdots,m\}$$

je ekvivalentan sljedećem problemu regularizirane regresije

$$\min_{\mathbf{x}\in\mathbb{R}^m}\left\{\|\mathbf{b}-A\mathbf{x}\|_a + \sum_{i=1}^{m} c_i\,|x_i|\right\}.$$

Zatim uklanjamo pretpostavku da su smetnje međusobno nepovezane. Dopuštanje ovisnih skupova nesigurnosti je korisno kada imamo dodatne informacije o potencijalnom šumu u problemu i želimo ograničiti konzervativnost formulacije najgoreg slučaja.
Razmotrimo sljedeći skup nesigurnosti:

$$\mathcal{U}' \coloneqq \left\{(\boldsymbol{\delta}_1,\cdots,\boldsymbol{\delta}_m) : f_j\left(\|\boldsymbol{\delta}_1\|_a,\cdots,\|\boldsymbol{\delta}_m\|_a\right) \leq 0;\, j=1,\cdots,k\right\},$$

gdje su f_j konveksne funkcije. Primijetimo da i k i f_j mogu biti proizvoljni, stoga je ovo vrlo općenita formulacija i daje nam značajnu fleksibilnost u dizajniranju skupova nesigurnosti i ekvivalentno novih regresijskih algoritama (vidi na primjer Korolare 2.3.3 i

2.3.4). Sljedeći teorem pokazuje da je ova robusna formulacija ekvivalentna općenitijem problemu regularizacijskog tipa, te stoga pretvara ovu formulaciju u problem optimizacije koji se može efikasno riješiti.

Teorem 2.3.2. *Pretpostavimo da skup $\mathcal{Z}$ koji definiramo na sljedeći način*

$$\mathcal{Z} := \left\{ z \in \mathbb{R}^m : f_j(\mathbf{z}) \leq 0, j = 1, \cdots, k; \mathbf{z} \geq \mathbf{0} \right\}$$

takav da vrijedi da postoji $\tilde{z} \in \mathcal{Z}$ tako da $f_j(\tilde{z}) < 0$ za svaku nelinearnu funkciju f_j, $j = 1, ..., k$.. Tada problem robusne regresije

$$\min_{\mathbf{x} \in \mathbb{R}^m} \left\{ \max_{\Delta A \in \mathcal{U}'} \|\mathbf{b} - (A + \Delta A)\mathbf{x}\|_a \right\}$$

je ekvivalentan sljedećem problemu regularizirane regresije.

$$\min_{\boldsymbol{\lambda} \in \mathbb{R}^k_+, \boldsymbol{\kappa} \in \mathbb{R}^m_+, \mathbf{x} \in \mathbb{R}^m} \left\{ \|\mathbf{b} - A\mathbf{x}\|_a + v(\boldsymbol{\lambda}, \boldsymbol{\kappa}, \mathbf{x}) \right\}, \tag{2.7}$$

gdje je

$$v(\boldsymbol{\lambda}, \boldsymbol{\kappa}, \mathbf{x}) \triangleq \max_{\mathbf{c} \in \mathbf{R}^m} \left[(\boldsymbol{\kappa} + |\mathbf{x}|)^\top \mathbf{c} - \sum_{j=1}^{k} \lambda_j f_j(\mathbf{c}) \right].$$

Dokaz. Fiksirajmo dopustivu točku, x^*.
Primijetimo da

$$\mathcal{U}' = \{(\boldsymbol{\delta}_1, \cdots, \boldsymbol{\delta}_m) : \mathbf{c} \in \mathcal{Z}; \|\boldsymbol{\delta}_i\|_a = c_i, i = 1, \cdots, m\}.$$

Zato imamo sljedeći raspis.

$$\begin{aligned} &\max_{\Delta A \in \mathcal{U}'} \|\mathbf{b} - (A + \Delta A)\mathbf{x}^*\|_a \\ &= \max_{\mathbf{c} \in \mathcal{Z}} \left\{ \max_{\|\delta_i\|_a = c_i, i = 1, \cdots, m} \|\mathbf{b} - (A + (\delta_1, \cdots, \delta_m))\, \mathbf{x}^*\|_a \right\} \\ &= \max_{\mathbf{c} \in \mathcal{Z}} \left\{ \|\mathbf{b} - A\mathbf{x}^*\|_a + \sum_{i=1}^{m} c_i \left| x_i^* \right| \right\} \\ &= \|\mathbf{b} - A\mathbf{x}^*\|_a + \max_{\mathbf{c} \in \mathcal{Z}} \left\{ |\mathbf{x}^*|^\top \mathbf{c} \right\}. \end{aligned} \tag{2.8}$$

Ovdje druga jednakost slijedi iz Teorema 2.3.1. Trebamo izračunati $\max_{\mathbf{c} \in \mathcal{Z}} \{|\mathbf{x}^*|^\top \mathbf{c}\}$ što je jednako $-\min_{\mathbf{c} \in \mathcal{Z}} \{-|\mathbf{x}^*|^\top \mathbf{c}\}$. Oznaka $|\mathbf{x}|$ nam označava vektor čije su komponente $|x_i|$.

Dakle, minimiziramo lineranu funkciju na konveksnom skupu. Po pretpostavci vrijede Slaterovi uvjeti. Stoga vrijedi rezultat jake dualnosti (vidi Teorem 5.2.13 u [3])

$$\min_{\mathbf{c}\in Z}\{-|\mathbf{x}^*|^T\mathbf{c}\} = \max_{\boldsymbol{\lambda}\in R^k_+,\boldsymbol{\kappa}\in R^m_+}\min_{\mathbf{c}\in R^m}\{-|\mathbf{x}^*|^T\mathbf{c} + \sum_{j=1}^{k}\boldsymbol{\lambda}_j f_j(\mathbf{c}) - \boldsymbol{\kappa}^T\mathbf{c}\},$$

odnosno

$$\max_{\mathbf{c}\in\mathcal{Z}}\left\{|\mathbf{x}^*|^\top\mathbf{c}\right\} = \min_{\boldsymbol{\lambda}\in\mathbb{R}^k_+,\boldsymbol{\kappa}\in\mathbb{R}^m_+} v\left(\boldsymbol{\lambda},\boldsymbol{\kappa},\mathbf{x}^*\right). \tag{2.9}$$

Tvrdnju teorema dobivamo tako da jednakost (2.9) ubacimo u jednakost (2.8) i minimiziramo po $\mathbf{x}^*$.

□

Sljedeća dva korolara su direktna primjena Teorema 2.3.2.

Korolar 2.3.3. *Neka je* $\mathcal{U}' = \{(\boldsymbol{\delta}_1,\cdots,\boldsymbol{\delta}_m) : ||||\boldsymbol{\delta}_1||_a,\cdots,||\boldsymbol{\delta}_m||_a||_s \le l;\}$ *za simetričnu normu* $||\cdot||_s$. *Tada je rezultirajući problem regularizirane regresije*

$$\min_{\mathbf{x}\in\mathbb{R}^m}\left\{||\mathbf{b}-A\mathbf{x}||_a + l||\mathbf{x}||_s^*\right\},$$

gdje je $||\cdot||_s^*$ *dualna norma od* $||\cdot||_s$.

Dokaz. Sad je skup $\mathcal{Z}$ zadan s

$$\mathcal{Z} = \{z\in\mathbb{R}^n : ||z||_s \le l, z\ge 0\}$$

pa možemo zaobići korištenje teorema jake dualnosti u prethodnom dokazu, već direktno riješiti primarnu zadaću. Zaista, zbog simetričnosti norme

$$\max_{\mathbf{c}\in Z}|\mathbf{x}|^T\mathbf{c} = \max_{||\mathbf{c}||_s\le l}\mathbf{x}^T\mathbf{c} = \max_{||\mathbf{c}||_s\le 1} l\mathbf{x}^T\mathbf{c} = l||\mathbf{x}||_s^*.$$

□

Korolar 2.3.4. *Neka je* $\mathcal{U}' = \left\{(\delta_1,\cdots,\delta_m) : \exists\mathbf{c}\ge 0 : T\mathbf{c}\le\mathbf{s}; \left\|\delta_j\right\|_a \le c_j;\right\}$ *za danu matricu* T *i vektor* $\mathbf{s}$. *Tada je regularizirani problem robusne regresije sljedeći optimizacijski problem po* x *i* λ*:*

$$\begin{aligned} \textit{Minimiziraj: } & ||\mathbf{b}-A\mathbf{x}||_a + \mathbf{s}^\top\boldsymbol{\lambda} \\ \textit{Uz uvjete: } & \mathbf{x} \le T^\top\boldsymbol{\lambda} \\ & -\mathbf{x} \le T^\top\boldsymbol{\lambda} \\ & \boldsymbol{\lambda}\ge\mathbf{0}. \end{aligned}$$

Za razliku od prethodnih rezultata, ovaj korolar uzima u obzir politope kao skupove nesigurnosti, tj ostvariva nesigurnost je ograničena, u smislu norme po stupcu, nekim elementom politopa $\{\mathbf{c} \geq 0 : T\mathbf{c} \leq \mathbf{s}\}$. U toj situaciji korišteni rezultat dualnosti svodi se na klasičnu dualnost u linearnom programiranju. Prednost takvih skupova je linearnost konačne formulacije. Štoviše, moć modeliranja je znatna budući da se na ovaj način mogu modelirati mnogi zanimljivi poremećaji.

2.4 Rijetkost

Rijetki algoritmi su algoritmi dizajnirani za rad sa strukturama podataka koje su rijetke, to jest većina podataka ima vrijednost nula ili vrijednost blizu nule. Cilj takvih algoritama je smanjenje vremenske i memorijske složenosti. U ovom odjeljku istražujemo svojstva rijetkosti rješenja zadaće robusne regresije (2.1) i, ekvivalentno, zadaće ℓ_1 regularizirane regresije, Lasso-a. Postoje dva pristupa za proučavanje Lasso zadaće. Prvi pristup istražuje problem iz statističke perspektive. To jest, pretpostavlja da su opažanja generirana (rijetkom) linearnom kombinacijom značajki i istražuje asimptotske ili vjerojatnosne uvjete potrebne da Lasso ispravno da generativni model. Generativni model u matematici je takav da može dati nove podatke koji su slični podacima za učenje. Model nauči vjerojatnosnu distribuciju podataka za učenje i onda koristi tu distribuciju kako bi generirao nove podatke. Drugi pristup promatra problem iz optimizacijske perspektive i proučava uvjete pod kojima par $(A, \mathbf{b})$ definira problem s rijetkim rješenjima.

Ovdje ćemo se baviti drugim pristupom te razmatramo uvjete koji dovode do toga da značajka dobije nultu težinu. Konkretno, pokazujemo da (i) mala promjena značajke kojoj je izvorno dodijeljena nulta težina i dalje dobiva nultu težinu, što je izravna posljedica neovisnosti skupa nesigurnosti među značajkama (Teorem 2.4.2); (ii) koristeći Teorem 2.4.2, pokazujemo da "gotovo" ortogonalne značajke imaju nultu težinu (Teorem 2.4.3). Slični rezultati kao u točki (ii), koji se oslanjaju na svojstvo nekoherentnosti, koriste se kao standardni alati u istraživanju rijetkosti Lasso-a iz statističke perspektive. Međutim, dokaz koji iskorištava svojstva nesigurnosti i robusnost je bitno drugačiji. Doista, takav dokaz pokazuje temeljnu vezu između robusnosti i rijetkosti i implicira da bi robustifikacija u odnosu na skup nesigurnosti neovisan u kontekstu značajki mogao biti koristan način za postizanje rijetkosti za druge probleme. Kako bismo naveli glavni teorem ovog odjeljka, iz kojeg proizlaze ostali rezultati, uvodimo neke oznake kako bismo olakšali raspravu.

Imamo podskup indeksa $I \subseteq \{1, \ldots, m\}$ i matricu ΔA. S ΔA^I označimo restrikciju ΔA na skup značajki I tako da ΔA^I je jednak ΔA na svakoj značajki s indeksom $i \in I$, dok je u ostalim slučajevima nula. Nadalje, imamo skup nesigurnosti $\mathcal{U}$ koji je neovisan u kontekstu značajki. Neka je $\mathcal{U}^I$ restrikcija od $\mathcal{U}$ na skup I tako da $\mathcal{U}^I \triangleq \left\{\Delta A^I \mid \Delta A \in \mathcal{U}\right\}$. Uočimo da svaki element $\Delta A \in \mathcal{U}$ se može zapisati kao $\Delta A^I + \Delta A^{I^c}$ (ovdje $I^c \triangleq \{1, \ldots, m\} \backslash I$) tako da $\Delta A^I \in \mathcal{U}^I$ i $\Delta A^{I^c} \in \mathcal{U}^{I^c}$.

Spomenimo još da je nosač funkcije f definiran kao zatvarač skupa $\{x \in D_f : f(x) \neq 0\}$. U skladu s tim za varijablu x kažemo da je nošena na nekom skupu indeksa I ako zadovoljava $x_j = 0, \forall j \notin I$.

Teorem 2.4.1. *Problem robusne regresije*

$$\min_{\mathbf{x}\in\mathbb{R}^m} \left\{ \max_{\Delta A \in \mathcal{U}} \|\mathbf{b} - (A + \Delta A)\mathbf{x}\|_2 \right\} \tag{2.10}$$

ima rješenje nošeno na skupu indeksa I ako postoji neka perturbacija $\Delta\tilde{A} \in \mathcal{U}^{I^c}$ *tako da problem robusne regresije*

$$\min_{\mathbf{x}\in\mathbb{R}^m} \left\{ \max_{\Delta A \in \mathcal{U}^I} \|\mathbf{b} - (A + \Delta\tilde{A} + \Delta A)\mathbf{x}\|_2 \right\} \tag{2.11}$$

ima rješenje nošeno na skupu I.

Dakle, robusna regresija ima rješenje nošeno na skupu I ako možemo pronaći jednu (ograničenu) perturbaciju značajki koje odgovaraju skupu I^c koja ih čini irelevantnima (tj. ne pridonose pogrešci regresije i stoga su s nultom težinom). Alternativno tumačenje je da ako je određena matrica ($A + \Delta\tilde{A}$ u teoremu) rijetka pod strožim uvjetom (imajte na umu da $\mathcal{U}^I$ favorizira težinu različitu od nule na I^c), tada su sve njene "susjedne" matrice rijetke pod blažim uvjetom. To dovodi do nove tehnike dokazivanja rijetkosti, identificiranjem "susjedne" matrice koja generira rijetka rješenja pod strogim uvjetima. Teorem 2.4.1 je zapravo poseban slučaj sljedećeg teorema s $c_j = 0$ za sve $j \notin I$.

Teorem 2.4.2. *Neka je* x^* *optimalno rješenje problema robusne regresije:*

$$\min_{\mathbf{x}\in\mathbb{R}^m} \left\{ \max_{\Delta A \in \mathcal{U}} \|\mathbf{b} - (A + \Delta A)\mathbf{x}\|_2 \right\} \tag{2.12}$$

i neka je x^* *nošeno na I,* $I \subseteq \{1, \cdots, m\}$*. Neka*

$$\tilde{\mathcal{U}} \coloneqq \left\{ (\delta_1, \cdots, \delta_m) \mid \|\delta_i\|_2 \leq c_i, \quad i \in I; \quad \left\|\delta_j\right\|_2 \leq c_j + l_j, j \notin I \right\}.$$

Tada je x^* *optimalno rješenje od*

$$\min_{\mathbf{x}\in\mathbb{R}^m} \left\{ \max_{\Delta A \in \tilde{\mathcal{U}}} \|\mathbf{b} - (\tilde{A} + \Delta A)\mathbf{x}\|_2 \right\} \tag{2.13}$$

za svaku $\tilde{A}$ *koja zadovoljava* $\left\|\tilde{\mathbf{a}}_j - \mathbf{a}_j\right\| \leq l_j$ *za* $j \notin I$ *te* $\tilde{\mathbf{a}}_i = \mathbf{a}_i$ *za* $i \in I$*.*

Dokaz. Primijetimo da vrijede sljedeće jednakosti:

$$\begin{aligned}
&\max_{\Delta A \in \tilde{\mathcal{U}}} \|\mathrm{b} - (A + \Delta A)\mathrm{x}^*\|_2 \\
&= \max_{\Delta A \in \mathcal{U}} \|\mathrm{b} - (A + \Delta A)\mathrm{x}^*\|_2 \\
&= \max_{\Delta A \in \mathcal{U}} \left\|\mathrm{b} - (\tilde{A} + \Delta A)\mathrm{x}^*\right\|_2 .
\end{aligned}$$

To vrijedi zato što za $j \notin I, x_j^* = 0$ tako da j-ti stupac od i ΔA i od $\tilde{A}$ nemaju utjecaj na rezidual.
Za proizvoljni x' imamo

$$\max_{\Delta A \in \mathcal{U}} \|\mathrm{b} - (A + \Delta A)\mathbf{x}'\|_2 \leq \max_{\Delta A \in \tilde{\mathcal{U}}} \left\|\mathrm{b} - (\tilde{A} + \Delta A)\mathrm{x}'\right\|_2 .$$

To vrijedi zato što $\left\|\mathbf{a}_j - \tilde{\mathbf{a}}_j\right\| \leq l_j$ za $j \notin I$ i $\mathbf{a}_i = \tilde{\mathbf{a}}_i$ za $i \in I$. Dakle, imamo

$$\{A + \Delta A \mid \Delta A \in \mathcal{U}\} \subseteq \{\tilde{A} + \Delta A \mid \Delta A \in \tilde{\mathcal{U}}\}.$$

Konačno, primijetimo da

$$\max_{\Delta A \in \mathcal{U}} \|\mathrm{b} - (A + \Delta A)\mathrm{x}^*\|_2 \leq \max_{\Delta A \in \mathcal{U}} \|\mathrm{b} - (A + \Delta A)\mathrm{x}'\|_2 .$$

Zato imamo

$$\max_{\Delta A \in \tilde{U}} \left\| \mathrm{b} - (\tilde{A} + \Delta A)\mathrm{x}^*\right\|_2 \leq \max_{\Delta A \in \tilde{\mathcal{U}}} \left\|\mathrm{b} - (\tilde{A} + \Delta A)\mathrm{x}'\right\|_2 .$$

Obzirom da to vrijedi za proizvoljan x', dokazali smo teorem. □

Sada možemo dokazati Teorem 2.4.1 koji je poseban slučaj Teorema 2.4.2 kojeg smo upravo dokazali.

Dokaz. Pokazujemo da je to poseban slučaj prethodnog teorema. Koristit ćemo ' za oznake iz Teorema 2.4.2. Imamo $\mathrm{b}, A, \mathcal{U}$ i I te radimo sljedeću konverziju

$$c_i' := c_i \quad , i \in I; \quad l_j' := c_j, c_j' := 0, \quad j \in I^c; \quad \tilde{A}' := A; \quad A' := A + \Delta\tilde{A}; \quad \mathbf{b}' := \mathbf{b}.$$

Zatim imamo

$$\begin{aligned}
\mathcal{U} &= \{(\delta_1, \cdots, \boldsymbol{\delta}_m) : \|\boldsymbol{\delta}_i\|_2 \leq c_i, \forall I\} \\
&= \left\{(\delta_1, \cdots, \delta_m) : \|\boldsymbol{\delta}_i\|_2 \leq c_i', \quad i \in I; \quad \left\|\boldsymbol{\delta}_j\right\|_2 \leq c_j' + l_j', j \notin I\right\} = \tilde{\mathcal{U}}'; \\
\mathcal{U}^I &= \left\{(\boldsymbol{\delta}_1, \cdots, \boldsymbol{\delta}_m) : \|\boldsymbol{\delta}_i\|_2 \leq c_i, \quad i \in I; \left\|\boldsymbol{\delta}_j\right\|_2 = 0, j \notin I\right\} \\
&= \left\{(\delta_1, \cdots, \delta_m) : \|\boldsymbol{\delta}_i\|_2 \leq c_i', \quad i \in I; \quad \left\|\boldsymbol{\delta}_j\right\|_2 \leq c_j', j \notin I\right\} = \mathcal{U}'; \\
\mathcal{U}^{I^c} &= \left\{(\delta_1, \cdots, \delta_m) : \|\delta_i\|_2 = 0, \quad i \in I; \left\|\boldsymbol{\delta}_j\right\|_2 \leq c_j, j \notin I\right\} \\
&= \left\{(\delta_1, \cdots, \delta_m) : \|\delta_i\|_2 = 0, \quad i \in I; \quad \left\|\delta_j\right\|_2 \leq l_j', j \notin I\right\}.
\end{aligned}$$

Dakle, problem (2.13) je ekvivalentan problemu (2.10) te je problem (2.12) ekvivalentan (2.11) Nadalje, $A' - \tilde{A}' = \Delta\tilde{A}$ implicira da $\left\|\tilde{\mathbf{a}}'_j - \mathbf{a}'_j\right\| \leq l'_j$ za $j \notin I$, i $\tilde{\mathbf{a}}'_i = \mathbf{a}'_i$ za $i \in I$ zbog činjenice da je $\Delta\tilde{A} \in \mathcal{U}^{I^c}$. Primjenom Teorema 2.4.2 slijedi tvrdnja. □

Pomnija analiza dokaza pokazuje da možemo zamijeniti ℓ_2 normu bilo kojom funkcijom gubitka f koja zadovoljava uvjet da ako je $x_j = 0$ te se A i A' razlikuju samo u j-tom stupcu, onda je $f(\mathrm{b}, A, \mathrm{x}) = f(\mathrm{b}, A', \mathrm{x})$. Ovaj teorem stoga predlaže metodologiju za konstruiranje rijetkih algoritama rješavanjem robusne optimizacije s obzirom na skupove nesigurnosti nepovezanih po stupcima.
Kada razmatramo ℓ_2 grešku, možemo prevesti uvjet da je značajka "irelevantna" u geometrijski uvjet, naime, ortogonalnost. Sada koristimo rezultat Teorema 2.4.1 da pokažemo da robusna regresija ima rijetko rješenje sve dok je zadovoljeno svojstvo tipa nekoherentnosti. Ovaj je rezultat više u skladu s tradicionalnim rezultatima rijetkosti, ali napominjemo da je geometrijsko razmišljanje drugačije, a naše se temelji na robusnosti. Doista, pokazujemo da značajka dobiva nultu težinu ako je "skoro" (tj. unutar dopuštene perturbacije) ortogonalna na signal i sve relevantne značajke.

Teorem 2.4.3. *Neka je $c_i = c$ te za sve i uzmimo ℓ_2 normu u definiciji skupa nesigurnosti. Pretpostavimo da postoji $I \subset \{1, \cdots, m\}$ takav da za sve $\mathbf{v} \in \mathrm{span}\left(\{\mathbf{a_i}, \mathbf{i} \in \mathrm{I}\} \bigcup \{\mathbf{b}\}\right), \|\mathbf{v}\| = 1$ imamo $\mathbf{v}^\top \mathbf{a}_j \leq c$, $j \notin I$. Tada postoji optimalno rješenje x^* koje je nošeno na I.*

Dokaz. Označimo za $j \notin I$ s $\mathbf{a}_j^=$ projekciju od a_j na skup svih linearnih kombinacija sljedećih vektora $\{\mathbf{a}_i, i \in I\} \bigcup \{\mathbf{b}\}$. I neka je $\mathbf{a}_j^+ \triangleq \mathbf{a}_j - \mathbf{a}_j^=$. Dakle, imamo $\left\|\mathbf{a}_j^=\right\| \leq c$. Neka je $\hat{A}$ takva da

$$\hat{\mathbf{a}}_i = \begin{cases} \mathbf{a}_i & i \in I \\ \mathbf{a}_i^+ & i \notin I \end{cases}$$

Sada, neka je

$$\hat{\mathcal{U}} \coloneqq \left\{(\delta_1, \cdots, \delta_m) : \|\delta_i\|_2 \leq c, i \in I; \left\|\delta_j\right\|_2 = 0, j \notin I\right\}.$$

Razmotrimo sljedeći problem robusne regresije $\min_{\hat{\mathbf{x}}} \left\{\max_{\Delta A \in \hat{\mathcal{U}}} \|\mathbf{b} - (\hat{A} + \Delta A)\hat{\mathbf{x}}\|_2\right\}$ koji je ekvivalentan $\min_{\hat{\mathrm{x}}} \left\{\|\mathbf{b} - \hat{A}\hat{\mathrm{x}}\|_2 + \sum_{i \in I} c\,|\hat{x}_i|\right\}$. Primijetimo da su $\hat{\mathrm{a}}_j$ ortogonalni na linearnu kombinaciju sljedećeg skupa vektora $\{\hat{\mathbf{a}}_i, i \in I\} \bigcup \{\mathbf{b}\}$. Dakle, za bilo koji $\hat{x}$, promjenom $\hat{x}_j$ na nulu za sve $j \notin I$ funkcija cilja koju minimiziramo se neće povećati. Budući da vrijedi $\left\|\hat{\mathbf{a}} - \hat{\mathbf{a}}_j\right\| = \left\|\mathbf{a}_j^=\right\| \leq c$, $j \notin I$, (uz $\mathcal{U} = \{(\delta_1, \cdots, \delta_m) : \|\delta_i\|_2 \leq c, i = 1, \ldots, m\}$), primjenom Teorema 2.4.2 dokazali smo tvrdnju. □

Kako bismo bolje razumjeli rezultate ovog odjeljka, možemo razmotriti generativni model $b = \sum_{i \in I} w_i a_i + \tilde{\xi}$ gdje je $I \subseteq \{1 \cdots, m\}$ te je $\tilde{\xi}$ proizvoljna varijabla šuma, to jest b je generiran značajkama iz I. Ako nadalje pretpostavimo da je vrijednost irelevantnih značajki (tj. značajki $\notin I$) slučajna varijabla s očekivanjem nula (recimo Gaussov šum),

slijedi da će, kako se broj uzoraka povećava, irelevantne značajke biti gotovo ortogonalne na potprostor obuhvaćen relevantnim značajkama i b s velikom vjerojatnošću. Posljedično, Lasso će irelevantnim značajkama dodijeliti nultu težinu.

2.5 Procjena gustoće i konzistentnost

U ovom odjeljku istražujemo formulaciju robusne linearne regresije iz statističke perspektive i ponovno izvodimo, koristeći samo svojstva robusnosti, da je Lasso asimptotski konzistentan. Osnovna ideja dokaza konzistentnosti je sljedeća. Pokazujemo da se robusna optimizacijska formulacija može smatrati maksimalnom pogreškom u odnosu na klasu mjera vjerojatnosti. Ova klasa uključuje procjenitelja gustoće jezgre, a pomoću njega pokazujemo da je Lasso konzistentan. Konzistentnost se odnosi na svojstvo procjenitelja gdje se procjenitelj približava pravoj vrijednosti parametra koji se procjenjuje kako se veličina uzorka povećava. To jest, kako se količina podataka poveća, procjenitelj postaje točniji.
Najprije predstavljamo neke pojmove i međurezultate. Konkretno, povezujemo robusnu optimizacijsku formulaciju s očekivanom korisnošću u najgorem slučaju (s obzirom na klasu mjera vjerojatnosti). Takvi će se rezultati koristiti za utvrđivanje konzistentnosti Lasso-a, kao i za pružanje nekih dodatnih uvida u robusnu optimizaciju. Kroz ovaj odjeljak koristimo $\mathcal{P}$ za predstavljanje skupa svih mjera vjerojatnosti na Borelovoj σ-algebri od $\mathbb{R}^{m+1}$.
Prvo utvrđujemo opći rezultat o ekvivalentnosti između robusne optimizacijske formulacije i očekivane korisnosti u najgorem slučaju.

Propozicija 2.5.1. *Za danu izmjerivu funkciju $f : \mathbb{R}^{m+1} \to \mathbb{R}$ i Borelove skupove $\mathcal{Z}_1, \cdots, \mathcal{Z}_n \subseteq \mathbb{R}^{m+1}$, neka je*

$$\mathcal{P}_n := \left\{ \mu \in \mathcal{P} : (\forall S \subseteq \{1, \cdots, n\})\, \mu\left(\bigcup_{i \in S} \mathcal{Z}_i \right) \geq \frac{|S|}{n} \right\}.$$

Tada vrijedi sljedeće:

$$\frac{1}{n} \sum_{i=1}^{n} \sup_{(\mathbf{r}_i, b_i) \in \mathcal{Z}_i} f\left(\mathbf{r}_i, b_i\right) = \sup_{\mu \in \mathcal{P}_n} \int_{\mathbb{R}^{m+1}} f(\mathbf{r}, b) d\mu(\mathbf{r}, b).$$

Kako bismo dokazali propoziciju, najprije iskažimo i dokažimo lemu.

Lema 2.5.2. *Ako imamo izmjerivu funkciju $f : \mathbb{R}^{m+1} \to \mathbb{R}$ i Borelov skup $\mathcal{Z} \subseteq \mathbb{R}^{m+1}$, vrijedi sljedeće:*

$$\sup_{\mathbf{x}' \in \mathcal{Z}} f\left(\mathbf{x}'\right) = \sup_{\mu \in \mathcal{P} | \mu(\mathcal{Z}) = 1} \int_{\mathbb{R}^{m+1}} f(\mathbf{x}) d\mu(\mathrm{x}).$$

Dokaz. Neka je $\hat{\mathbf{x}}$ $\epsilon-$ optimalno rješenje lijeve strane, uzimajući u obzir vjerojatnosnu mjeru μ' koja stavlja težinu 1 na $\hat{\mathbf{x}}$. Imamo

$$\sup_{\mathbf{x}' \in \mathcal{Z}} f(\mathbf{x}') - \epsilon \leq \sup_{\mu \in \mathcal{P} | \mu(\mathcal{Z})=1} \int_{\mathbb{R}^{m+1}} f(\mathbf{x}) d\mu(\mathbf{x}),$$

obzirom da ϵ može biti proizvoljno mali što vodi do

$$\sup_{\mathbf{x}' \in \mathcal{Z}} f(\mathrm{x}') \leq \sup_{\mu \in \mathcal{P} | \mu(\mathcal{Z})=1} \int_{\mathbb{R}^{m+1}} f(\mathrm{x}) d\mu(\mathrm{x}). \tag{2.14}$$

Nadalje, konstruirajmo funkciju $\hat{f} : \mathbb{R}^{m+1} \to \mathbb{R}$ na sljedeći način

$$\hat{f}(\mathrm{x}) := \begin{cases} f(\hat{\mathrm{x}}) & \mathrm{x} \in \mathcal{Z} \\ f(\mathrm{x}) & \text{inače.} \end{cases}$$

Po definiciji od $\hat{\mathrm{x}}$ vrijedi $f(x) \leq \hat{f}(\mathrm{x}) + \epsilon$ za sve $\mathbf{x} \in \mathbb{R}^{m+1}$. Zato vrijedi sljedeće za svaku vjerojatnosnu mjeru μ takvu da $\mu(\mathcal{Z}) = 1$

$$\int_{\mathbb{R}^{m+1}} f(\mathrm{x}) d\mu(x) \leq \int_{\mathbb{R}^{m+1}} \hat{f}(\mathrm{x}) d\mu(x) + \epsilon = f(\hat{\mathbf{x}}) + \epsilon \leq \sup_{\mathbf{x}' \in \mathcal{Z}} f(\mathbf{x}') + \epsilon$$

što vodi do

$$\sup_{\mu \in \mathcal{P} | \mu(\mathcal{Z})=1} \int_{\mathbb{R}^{m+1}} f(\mathbf{x}) d\mu(x) \leq \sup_{\mathbf{x}' \in \mathcal{Z}} f(\mathbf{x}') + \epsilon.$$

Kako ϵ može biti proizvoljno mali, imamo

$$\sup_{\mu \in \mathcal{P} | \mu(\mathcal{Z})=1} \int_{\mathbb{R}^{m+1}} f(\mathbf{x}) d\mu(x) \leq \sup_{\mathbf{x}' \in \mathcal{Z}} f(\mathbf{x}'). \tag{2.15}$$

Kombinirajući (2.14) i (2.15), dokazali smo lemu.

□

Sada dokažimo Propoziciju 2.5.1.

Dokaz. Neka je $\hat{\mathbf{x}}_i$ ϵ-optimalno rješenje od $\sup_{\mathbf{x}_i \in \mathcal{Z}_i} f(\mathbf{x}_i)$. Primijetimo da empirijska distribucija za $(\hat{\mathbf{x}}_1, \cdots, \hat{\mathbf{x}}_n)$ pripada $\mathcal{P}_n$ obzirom da ϵ može biti proizvoljno blizu 0 pa imamo

$$\frac{1}{n} \sum_{i=1}^{n} \sup_{\mathbf{x}_i \in \mathcal{Z}_i} f(\mathrm{x}_i) \leq \sup_{\mu \in \mathcal{P}_n} \int_{\mathbb{R}^{m+1}} f(\mathrm{x}) d\mu(\mathrm{x}). \tag{2.16}$$

Bez smanjenja općenitosti možemo pretpostaviti

$$f(\hat{\mathrm{x}}_1) \leq f(\hat{\mathrm{x}}_2) \leq \cdots \leq f(\hat{\mathrm{x}}_n). \tag{2.17}$$

Sada konstruirajmo sljedeću funkciju

$$\hat{f}(\mathrm{x}) := \begin{cases} \min_{i|\mathbf{x}\in\mathcal{Z}_i} f(\hat{\mathbf{x}}_i) & \mathbf{x} \in \bigcup_{j=1}^{n} \mathcal{Z}_j \\ f(\mathbf{x}) & \text{inače} \end{cases} \tag{2.18}$$

i primijetimo da $f(\mathrm{x}) \leq \hat{f}(\mathrm{x}) + \epsilon$ za sve x.
Nadalje, obzirom $\mu \in \mathcal{P}_n$, imamo

$$\begin{aligned} &\int_{\mathbb{R}^{m+1}} f(\mathrm{x}) d\mu(\mathrm{x}) - \epsilon \\ &= \int_{\mathbb{R}^{m+1}} \hat{f}(\mathrm{x}) d\mu(\mathrm{x}) \\ &= \sum_{k=1}^{n} f(\hat{\mathbf{x}}_k) \left[\mu\left(\bigcup_{i=1}^{k} \mathcal{Z}_i \right) - \mu\left(\bigcup_{i=1}^{k-1} \mathcal{Z}_i \right) \right]. \end{aligned}$$

Označimo $\alpha_k := \left[\mu\left(\bigcup_{i=1}^{k} \mathcal{Z}_i \right) - \mu\left(\bigcup_{i=1}^{k-1} \mathcal{Z}_i \right) \right]$ pa imamo

$$\sum_{k=1}^{n} \alpha_k = 1, \quad \sum_{k=1}^{t} \alpha_k \geq t/n.$$

Zbog (2.17) imamo

$$\sum_{k=1}^{n} \alpha_k f(\hat{\mathbf{x}}_k) \leq \frac{1}{n} \sum_{k=1}^{n} f(\hat{\mathbf{x}}_k).$$

Dakle, za svaki $\mu \in \mathcal{P}_n$ je

$$\int_{\mathbb{R}^{m+1}} f(\mathrm{x}) d\mu(\mathrm{x}) - \epsilon \leq \frac{1}{n} \sum_{k=1}^{n} f(\hat{\mathrm{x}}_k).$$

Zato

$$\sup_{\mu\in\mathcal{P}_n} \int_{\mathbb{R}^{m+1}} f(\mathrm{x}) d\mu(\mathrm{x}) - \epsilon \leq \sup_{\mathrm{x}_i\in\mathcal{Z}_i} \frac{1}{n} \sum_{k=1}^{n} f(\mathrm{x}_k).$$

Zbog (2.16) i kako je ϵ proizvoljno blizu 0, dokazali smo propoziciju.

□

To dovodi do sljedećeg korolara za Lasso, koji kaže da je za dani x, robusni regresijski gubitak jednak očekivanoj pogrešci u najgorem slučaju.

Korolar 2.5.3. *Za dane* $\mathbf{b} \in \mathbb{R}^n, A \in \mathbb{R}^{n\times m}$ *sljedeća jednakost vrijedi za svaki* $\mathrm{x} \in \mathbb{R}^m$.

$$\|\mathbf{b} - A\mathbf{x}\|_2 + \sqrt{n}c_n\|\mathbf{x}\|_1 + \sqrt{n}c_n = \sup_{\mu\in\hat{\mathcal{P}}(n)} \sqrt{n \int_{\mathbb{R}^{m+1}} (b' - \mathbf{r}'^{\top}\mathbf{x})^2 \, d\mu(\mathbf{r}', b')}. \tag{2.19}$$

Ovdje je

$$\hat{\mathcal{P}}(n) := \bigcup_{\|\boldsymbol{\sigma}\|_2 \le \sqrt{n}c_n; \forall i: \|\boldsymbol{\delta}_i\|_2 \le \sqrt{n}c_n} \mathcal{P}_n(A, \Delta, \mathbf{b}, \boldsymbol{\sigma});$$

$$\mathcal{P}_n(A, \Delta, \mathbf{b}, \boldsymbol{\sigma}) := \left\{ \mu \in \mathcal{P} : \mathcal{Z}_i = [b_i - \sigma_i, b_i + \sigma_i] \times \prod_{j=1}^{m} \left[a_{ij} - \delta_{ij}, a_{ij} + \delta_{ij} \right] ; \right.$$

$$\left. \forall S \subseteq \{1, \cdots, n\} : \mu\left(\bigcup_{i \in S} \mathcal{Z}_i \right) \ge \frac{|S|}{n} \right\}.$$

Dokaz. Desna strane jednakosti (2.19) je jednaka sljedećem izrazu

$$\sup_{\|\boldsymbol{\sigma}\|_2 \le \sqrt{n}c_n; \forall i: \|\boldsymbol{\delta}_i\|_2 \le \sqrt{n}c_n} \left\{ \sup_{\mu \in \mathcal{P}_n(A, \Delta, \mathbf{b}, \boldsymbol{\sigma})} \sqrt{n \int_{\mathbb{R}^{m+1}} (b' - \mathbf{r}'^{\top}\mathbf{x})^2 \, d\mu\,(\mathbf{r}', b')} \right\}.$$

Primijetimo da po ekvivalenciji robusnoj formulaciji lijeva strana je jednaka

$$\begin{aligned}
&\max_{\|\boldsymbol{\sigma}\|_2 \le \sqrt{n}c_n; \forall i: \|\boldsymbol{\delta}_i\|_2 \le \sqrt{n}c_n} \|\mathbf{b} + \boldsymbol{\sigma} - (A + [\boldsymbol{\delta}_1, \cdots, \delta_m])\,\mathbf{x}\|_2 \\
&= \sup_{\|\boldsymbol{\sigma}\|_2 \le \sqrt{n}c_n; \forall i: \|\boldsymbol{\delta}_i\|_2 \le \sqrt{n}c_n} \left\{ \sup_{(\hat{b}_i, \hat{\mathbf{r}}_i) \in [b_i - \sigma_i, b_i + \sigma_i] \times \prod_{j=1}^{m} [a_{ij} - \delta_{ij}, a_{ij} + \delta_{ij}]} \sqrt{\sum_{i=1}^{n} \left(\hat{b}_i - \hat{\mathbf{r}}_i^{\top}\mathbf{x} \right)^2} \right\} \\
&= \sup_{\|\boldsymbol{\sigma}\|2 \le \sqrt{n}c_n; \forall i: \|\boldsymbol{\delta}_i\|_2 \le \sqrt{n}c_n} \sqrt{\sum_{i=1}^{n} \sup_{(\hat{b}_i, \hat{\mathbf{r}}_i) \in [b_i - \sigma_i, b_i + \sigma_i] \times \prod_{j=1}^{m} [a_{ij} - \delta_{ij}, a_{ij} + \delta_{ij}]} \left(\hat{b}_i - \hat{\mathbf{r}}_i^{\top}\mathbf{x} \right)^2}.
\end{aligned}$$

Nadalje, primjenom 2.5.1 slijedi

$$\begin{aligned}
&\sqrt{\sum_{i=1}^{n} \sup_{(\hat{b}_i, \hat{\mathbf{r}}_i) \in [b_i - \sigma_i, b_i + \sigma_i] \times \prod_{j=1}^{m} [a_{ij} - \delta_{ij}, a_{ij} + \delta_{ij}]} \left(\hat{b}_i - \hat{\mathbf{r}}_i^{\top}\mathbf{x} \right)^2} \\
&= \sqrt{\sup_{\mu \in \mathcal{P}_n(A, \Delta, \mathbf{b}, \boldsymbol{\sigma})} n \int_{\mathbb{R}^{m+1}} (b' - \mathbf{r}'^{\top}\mathbf{x})^2 \, d\mu\,(\mathbf{r}', b')} \\
&= \sup_{\mu \in \mathcal{P}_n(A, \Delta, \mathbf{b}, \boldsymbol{\sigma})} \sqrt{n \int_{\mathbb{R}^{m+1}} (b' - \mathbf{r}'^{\top}\mathbf{x})^2 \, d\mu\,(\mathbf{r}', b')}
\end{aligned}$$

što dokazuje korolar. □

Pružimo dodatno značenje Korolara 2.5.3. Jednadžba (2.19) nije vjerojatnosna. To jest, vrijedi bez ikakve pretpostavke (npr. nezavisnost i jednaka distribuiranost ili generiranost određenim distribucijama) o b i A i ne uključuje nikakvu probabilističku operaciju kao što je uzimanje očekivanja na lijevoj strani. Umjesto toga, to je odnos ekvivalencije koji vrijedi za proizvoljan skup uzoraka. Imajmo na umu da desna strana također ovisi o uzorcima jer je $\hat{\mathcal{P}}(n)$ definiran kroz A i b. Doista, $\hat{\mathcal{P}}(n)$ predstavlja uniju klasa distribucija $\mathcal{P}_n(A, \Delta, \mathbf{b}, \boldsymbol{\sigma})$ tako da je norma svakog stupca od Δ ograničena, gdje je $\mathcal{P}_n(A, \Delta, \mathbf{b}, \boldsymbol{\sigma})$ skup distribucije koje odgovaraju (vidi Propoziciju 2.5.1) poremećaju u hiperpravokutnim Borelovim skupovima $\mathcal{Z}_1, \cdots, \mathcal{Z}_n$ sa središtem na $\left(b_i, \mathbf{r}_i^\top\right)$ s duljinama $(2\sigma_i, 2\delta_{i1}, \cdots, 2\delta_{im})$.
Dokaz konzistentnosti oslanja se na dokazivanje da ovaj skup $\hat{\mathcal{P}}(n)$ distribucija sadrži procjenitelj gustoće jezgre.

Definicija 2.5.4. *Procjenitelj gustoće jezgre za gustoću $\hat{h} \in \mathbb{R}^d$ definira se kao*

$$h_n(\mathbf{x}) = \left(nc_n^d\right)^{-1} \sum_{i=1}^{n} K\left(\frac{\mathbf{x} - \hat{\mathbf{x}}_i}{c_n}\right),$$

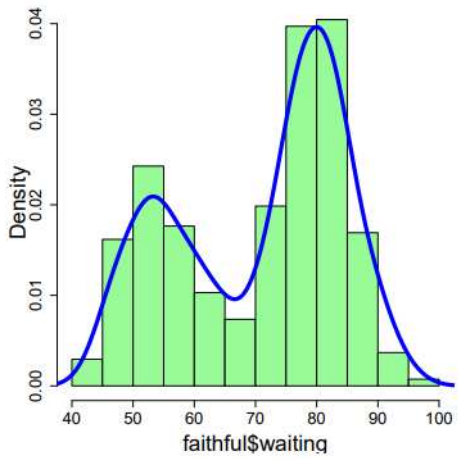
gdje je c_n niz pozitivnih brojeva, $\hat{\mathbf{x}}_i$ su uzorci generirani prema $\hat{f}$, a K je Borelova izmjeriva funkcija (jezgra) koja zadovoljava $K \geq 0$, $\int K = 1$.

Slika 2.3 prikazuje procjenitelj gustoće jezgre i histogram skupa podataka u R-u. Plava krivulja je krivulja gustoće procijenjena pomoću procjenitelja gustoće jezgre.

Sada, imamo tri jezgrene funkcije: Gaussovu $K(x) = \frac{1}{\sqrt{2\pi}} e^{\frac{-x^2}{2}}$, uniformnu $K(x) = \frac{1}{2} I(-1 \leq x \leq 1)$, Epanechnikovu $K(x) = \frac{3}{4} \cdot \max\left\{1 - x^2, 0\right\}$.

Na slici 2.4 gornji red prikazuje tri funkcije jezgre, a donji red prikazuje odgovarajuće procjenitelje gustoće na istom skupu podataka kao i na prethodnoj slici.

Što se tiče konzistentnosti od Lasso-a, ograničavamo našu raspravu na slučaj kada je veličina dopuštene nesigurnosti za sve značajke jednaka c, (tj. standardni Lasso) i utvrđujemo statističku konzistentnost Lasso-a iz argumenta distribucijske robusnosti. Generalizacija na neuniformni slučaj je jednostavna. Cijelo vrijeme koristimo c_n za predstavljanje c gdje postoji n uzoraka (c_n teži u nulu).
Prisjetimo se standardnog generativnog modela u statističkom učenju: neka je $\mathbb{P}$ mjera vjerojatnosti takva da dodjeljuje vjerojatnosti konačnom broju točaka (ili prebrojivom) koja generira uzorke $(b_i, \mathbf{r}_i)$, te ima gustoću f^*. Označimo skup od prvih n uzoraka sa $\mathcal{S}_n$. Defi-



Slika 2.3: Histogram i krivulja gustoće

nirajmo

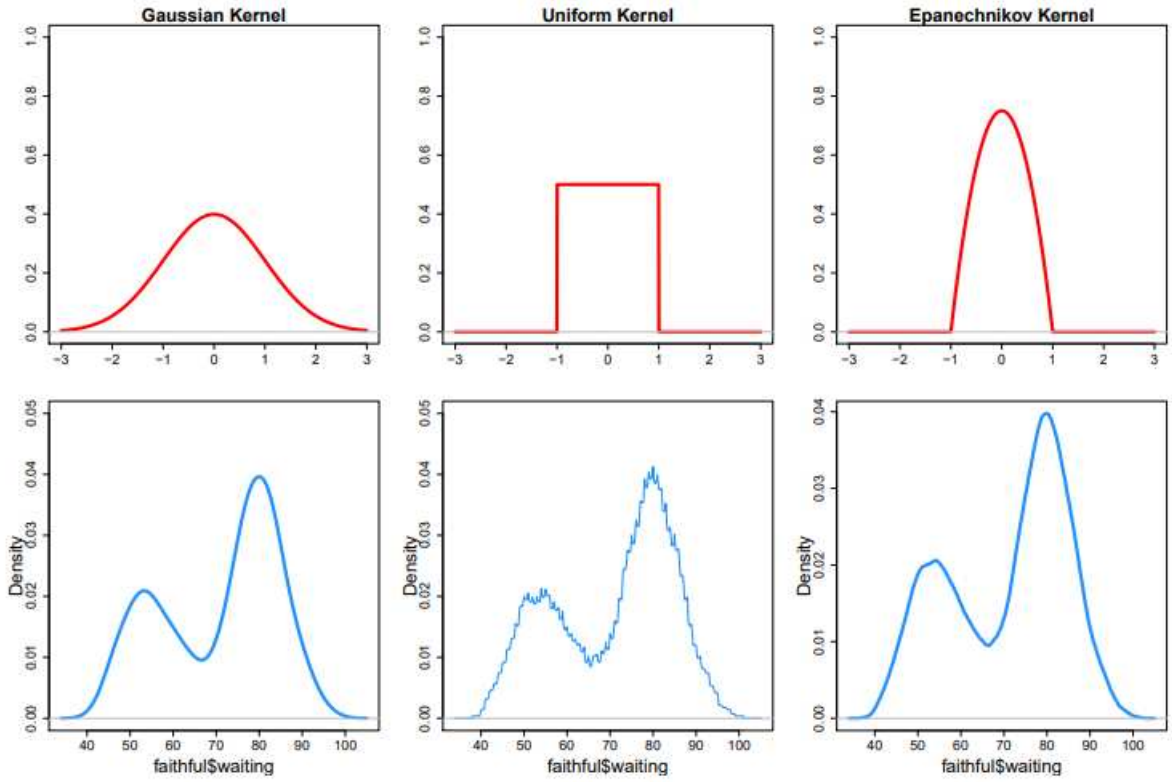
$$\mathbf{x}(c_n, \mathcal{S}_n) := \arg\min_{\mathbf{x}} \left\{ \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(b_i - \mathbf{r}_i^\top \mathbf{x}\right)^2} + c_n\|x\|_1 \right\}$$

$$= \arg\min_{\mathbf{x}} \left\{ \frac{\sqrt{n}}{n}\sqrt{\sum_{i=1}^{n}\left(b_i - \mathbf{r}_i^\top \mathbf{x}\right)^2} + c_n\|x\|_1 \right\},$$

$$\mathbf{x}(\mathbb{P}) := \arg\min_{\mathbf{x}} \left\{ \sqrt{\int_{b,\mathbf{r}} (b - \mathbf{r}^\top \mathbf{x})^2 \, d\mathbb{P}(b, \mathbf{r})} \right\}.$$

Riječima, $\mathbf{x}(c_n, \mathcal{S}_n)$ je rješenje za Lasso s parametrom kompromisa postavljenim na $c_n\sqrt{n}$, a $\mathbf{x}(\mathbb{P})$ je "pravo" optimalno rješenje.

Imamo sljedeći rezultat konzistentnosti. Sam teorem dobro je poznat rezultat. Međutim, tehnika dokazivanja je nova. Ova je tehnika zanimljiva jer standardne tehnike za utvrđivanje dosljednosti u statističkom učenju, uključujući Vapnik–Chervonenkisovu dimenziju i algoritamsku stabilnost često funkcioniraju za ograničen raspon algoritama. Na primjer, poznato je da k-najbliži susjed ima beskonačnu Vapnik–Chervonenkisovu dimenziju, a kasnije pokazujemo da Lasso nije stabilan. Nasuprot tome, puno širi raspon algoritama ima interpretacije robusnosti, što omogućuje jedinstven pristup da se dokaže njihova dosljednost.



Slika 2.4: Jezgrene funkcije

Teorem 2.5.5. *Neka je c_n takav da vrijedi $c_n \downarrow 0$ i $\lim_{n\to\infty} n\,(c_n)^{m+1} = \infty$. Pretpostavimo da postoji konstanta takva da $\|\mathbf{x}\,(c_n, \mathcal{S}_n)\|_2 \leq H$ za svaki n. Tada*

$$\lim_{n\to\infty} \sqrt{\int_{b,\mathbf{r}} (b - \mathbf{r}^\top \mathbf{x}\,(c_n, \mathcal{S}_n))^2 \, d\mathbb{P}(b, \mathbf{r})} = \sqrt{\int_{b,\mathbf{r}} (b - \mathbf{r}^\top \mathbf{x}(\mathbb{P}))^2 \, d\mathbb{P}(b, \mathbf{r})},$$

gotovo sigurno.

Dokaz. **Prvi korak:** Pokazujemo da desna strana jednakosti (2.19) uključuje procjenitelj gustoće jezgre za pravu, ali nepoznatu distribuciju. Razmotrimo sljedeći procjenitelj jezgre danih uzoraka $\mathcal{S}_n = (b_i, \mathbf{r}_i)_{i=1}^n$ i kompromisnog parametra c_n:

$$f_n(b, \mathbf{r}) \triangleq \left(n c_n^{m+1}\right)^{-1} \sum_{i=1}^{n} K\left(\frac{b - b_i, \mathbf{r} - \mathbf{r}_i}{c_n}\right)$$

$$\text{gdje: } K(\mathbf{z}) \triangleq I_{[-1,+1]^{m+1}}(\mathbf{z})/2^{m+1}. \tag{2.20}$$

Drugi korak: Koristeći svojstvo $\mathcal{L}^1$ konvergencije procjenitelja gustoće jezgre, dokazujemo konzistentnost robusne regresije i ekvivalentno Lasso.
Najprije primijetimo činjenicu da vrijedi $\|\mathbf{x}(c_n, \mathcal{S}_n)\|_2 \leq H$ i imamo $\mathbb{P}$ koja dodjeljuje vjerojatnosti konačnom broju točaka (ili prebrojivom). To implicira da postoji univerzalna konstanta C takva da

$$\max_{(b,\mathbf{r})\in\text{nosač}(\mathbb{P})} \left(b - \mathbf{r}^\top \mathbf{x}(c_n, \mathcal{S}_n)\right)^2 \leq C.$$

Po Korolaru 2.5.3 i budući da vrijedi $\hat{\mu}_n \in \hat{\mathcal{P}}(n)$, imamo:

$$\begin{aligned}
&\sqrt{\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}(c_n, \mathcal{S}_n)\right)^2 d\hat{\mu}_n(b, \mathbf{r})} \\
&\leq \sup_{\mu\in\hat{\mathcal{P}}(n)} \sqrt{\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}(c_n, \mathcal{S}_n)\right)^2 d\mu(b, \mathbf{r})} \\
&= \frac{\sqrt{n}}{n} \sqrt{\sum_{i=1}^{n} \left(b_i - \mathbf{r}_i^\top \mathbf{x}(c_n, \mathcal{S}_n)\right)^2} + c_n \|\mathbf{x}(c_n, \mathcal{S}_n)\|_1 + c_n \\
&\leq \frac{\sqrt{n}}{n} \sqrt{\sum_{i=1}^{n} \left(b_i - \mathbf{r}_i^\top \mathbf{x}(\mathbb{P})\right)^2} + c_n \|\mathbf{x}(\mathbb{P})\|_1 + c_n,
\end{aligned}$$

gdje zadnja nejednakost proizlazi iz definicije $\mathbf{x}(c_n, \mathcal{S}_n)$.

Kad kvadriramo obje strane, imamo

$$\begin{aligned}
&\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}(c_n, \mathcal{S}_n)\right)^2 d\hat{\mu}_n(b, \mathbf{r}) \\
&\leq \frac{1}{n} \sum_{i=1}^{n} \left(b_i - \mathbf{r}_i^\top \mathbf{x}(\mathbb{P})\right)^2 + c_n^2 \left(1 + \|\mathbf{x}(\mathbb{P})\|_1\right)^2 \\
&+ 2c_n \left(1 + \|\mathbf{x}(\mathbb{P})\|_1\right) \sqrt{\frac{1}{n} \sum_{i=1}^{n} \left(b_i - \mathbf{r}_i^\top \mathbf{x}(\mathbb{P})\right)^2}.
\end{aligned}$$

Primijetimo da desna strana konvergira k $\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}(\mathbb{P})\right)^2 d\mathbb{P}(b, \mathbf{r})$ kad $n \uparrow \infty$ i $c_n \downarrow 0$

gotovo sigurno. Nadalje, imamo

$$\begin{aligned}
&\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\mathbb{P}(b,\mathbf{r}) \\
&\leq \int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\hat{\mu}_n(b,\mathbf{r}) \\
&\quad + \left[\max_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2\right] \int_{b,\mathbf{r}} \left|f_n(b,\mathbf{r}) - f^*(b,\mathbf{r})\right| d(b,\mathbf{r}) \\
&\leq \int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\hat{\mu}_n(b,\mathbf{r}) + C \int_{b,\mathbf{r}} \left|f_n(b,\mathbf{r}) - f^*(b,\mathbf{r})\right| d(b,\mathbf{r}),
\end{aligned}$$

gdje zadnja nejednakost slijedi iz definicije od C. Uočimo da $\int_{b,\mathbf{r}} |f_n(b,\mathbf{r}) - f^*(b,\mathbf{r})|\, d(b,\mathbf{r})$ ide u nulu gotovo sigurno kad $c_n \downarrow 0$ i $nc_n^{m+1} \uparrow \infty$ budući da $f_n(\cdot)$ je procjenitelj gustoće jezgre od $f^*(\cdot)$. Dakle, tvrdnja teorema slijedi. □

Možemo maknuti pretpostavku da $\|\mathbf{x}\left(c_n, \mathcal{S}_n\right)\|_2 \leq H$ i, kao u Teoremu 2.5.5, tehnika dokazivanja nam je zanimljivija od samog rezultata.

Teorem 2.5.6. *Neka c_n konvergira nuli dovoljno sporo. Tada vrijedi*

$$\lim_{n\to\infty} \sqrt{\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\mathbb{P}(b,\mathbf{r})} = \sqrt{\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}(\mathbb{P})\right)^2 d\mathbb{P}(b,\mathbf{r})},$$

gotovo sigurno.

Kako bismo dokazali teorem, najprije moramo razmotriti skup distribucija koje pripadaju $\hat{\mathcal{P}}(n)$. Zato ćemo najprije dokazati sljedeću lemu.

Lema 2.5.7. *Podijelimo nosač od $\mathbb{P}$ na $V_1, \cdots, V_T$ tako da ℓ^∞ radijus svakog skupa je manji od c_n. Ako distribucija μ zadovoljava*

$$\mu\left(V_t\right) = \frac{\left|\{i \mid (b_i, \mathbf{r}_i) \in V_t\}\right|}{n}; \quad t = 1, \cdots, T, \tag{2.21}$$

onda je $\mu \in \hat{\mathcal{P}}(n)$.

Dokaz. Neka $\mathcal{Z}_i = [b_i - c_n, b_i + c_n] \times \prod_{j=1}^m \left[a_{ij} - c_n, a_{ij} + c_n\right]$ gdje je a_{ij} j-ti element od $\mathbf{r}_i$. Imamo

$$(b_i, \mathbf{r}_i) \in V_t \Rightarrow V_t \subseteq \mathcal{Z}_i.$$

Za svaki $S \subseteq \{1, \cdots, n\}$ vrijedi:

$$\begin{aligned}
&\mu\left(\bigcup_{i\in S} \mathcal{Z}_i\right) \geq \mu\left(\bigcup V_t : \exists i \in S : b_i, \mathbf{r}_i \in V_t\right) \\
&= \sum_{\exists i\in S : b_i, \mathbf{r}_i \in V_t} \mu\left(V_t\right) = \sum_{t \mid \exists i \in S : b_i, \mathbf{r}_i \in V_t} \#\left(\left(b_i, \mathbf{r}_i\right) \in V_t\right)/n \geq |S|/n.
\end{aligned}$$

Dakle, $\mu \in \mathcal{P}_n\left(A, \Delta, b, c_n\right)$ gdje svaki element od Δ je c_n što vodi do toga da je $\mu \in \hat{\mathcal{P}}(n)$. □

Budući da smo dokazali lemu, možemo se vratiti dokazu prethodnog teorema.

Dokaz. Podijelimo nosač od $\mathbb{P}$ na T podskupova tako da ℓ^∞ radijus od svakog je manji od c_n. Označimo s $\tilde{\mathcal{P}}(n)$ skup mjera vjerojatnosti koje zadovoljavaju jednakost (2.21). Stoga, $\tilde{\mathcal{P}}(n) \subseteq \hat{\mathcal{P}}(n)$ po prethodnoj lemi. Nadalje primijetite da postoji univerzalna konstanta K takva da je$\|\mathbf{x}\left(c_n, \mathcal{S}_n\right)\|_2 \leq K/c_n$ zbog činjenice da je kvadratni gubitak rješenja $x = 0$ ograničen konstantom koja ovisi samo o nosaču od $\mathbb{P}$. Dakle, postoji konstanta C takva da vrijedi $\max_{b,\mathbf{r}}\left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 \leq C/c_n^2$.
Analogno kao kod dokaza Teorema 2.5.5, imamo

$$\begin{aligned}
&\sup_{\mu_n \in \tilde{\mathcal{P}}(n)} \int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\mu_n(b, \mathbf{r}) \\
&\leq \frac{1}{n}\sum_{i=1}^{n} \left(b_i - \mathbf{r}_i^\top \mathbf{x}(\mathbb{P})\right)^2 + c_n^2\left(1 + \|\mathbf{x}(\mathbb{P})\|_1\right)^2 \\
&\quad + 2c_n\left(1 + \|\mathbf{x}(\mathbb{P})\|_1\right)\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(b_i - \mathbf{r}_i^\top \mathbf{x}(\mathbb{P})\right)^2},
\end{aligned} \tag{2.22}$$

te

$$\begin{aligned}
&\int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\mathbb{P}(b, \mathbf{r}) \\
&\leq \inf_{\mu_n \in \tilde{\mathcal{P}}(n)} \left\{ \int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\mu_n(b, \mathbf{r}) \right. \\
&\left. + \max_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 \int_{b,\mathbf{r}} \left|f_{\mu_n}(b, \mathbf{r}) - f(b, \mathbf{r})\right| d(b, \mathbf{r}) \right\} \\
&\leq \sup_{\mu_n \in \tilde{\mathcal{P}}(n)} \int_{b,\mathbf{r}} \left(b - \mathbf{r}^\top \mathbf{x}\left(c_n, \mathcal{S}_n\right)\right)^2 d\mu_n(b, \mathbf{r}) \\
&+ 2C/c_n^2 \inf_{\mu_n' \in \tilde{\mathcal{P}}(n)} \left\{ \int_{b,\mathbf{r}} \left|f_{\mu_n'}(b, \mathbf{r}) - f(b, \mathbf{r})\right| d(b, \mathbf{r}) \right\},
\end{aligned}$$

gdje f_μ predstavlja funkciju gustoće mjere μ. Primijetimo da je $\tilde{\mathcal{P}}_n$ skup distribucija koje zadovoljavaju jednakost (2.21). Zato je $\inf_{\mu'_n \in \tilde{\mathcal{P}}(n)} \int_{b,\mathbf{r}} \left| f_{\mu'_n}(b, \mathbf{r}) - f(b, \mathbf{r}) \right| d(b, \mathbf{r})$ odozgo ograničen s $\sum_{t=1}^{T} \left| \mathbb{P}(V_t) - \#(b_i, \mathbf{r}_i \in V_t) \right| / n$ što teži u nulu kako se n povećava za neki fiksni c_n. Zato

$$2C/c_n^2 \inf_{\mu'_n \in \tilde{\mathcal{P}}(n)} \left\{ \int_{b,\mathbf{r}} \left| f_{\mu'_n}(b, \mathbf{r}) - f(b, \mathbf{r}) \right| d(b, \mathbf{r}) \right\} \to 0$$

ako $c_n \downarrow 0$ dovoljno sporo. Zajedno s nejednakosti (2.22), ovo dokazuje tvrdnju teorema. □

2.6 Stabilnost

Obzirom da znamo da problem robusne regresije, a posebno Lasso, potiču rijetkost, zanimljivo je istražiti još jednu poželjnu karakteristiku algoritma učenja, naime radi se o stabilnosti. U statistici se Lasso smatra nestabilnim ako male promjene u podacima korištenim za prilagođavanje modela mogu dovesti do velikih promjena u procijenjenim parametrima. To može predstavljati problem jer znači da procjene koje proizvodi Lasso model mogu biti vrlo osjetljive na male varijacije u podacima i možda neće biti vrlo pouzdane. U ovom dijelu pokazujemo da Lasso nije stabilan.

Prije davanja formalnih definicija, ukratko ćemo komentirati razliku između pojmova robusnost i stabilnost. U ovom radu, "robusnost" označava svojstvo algoritma da će njegova izlazna regresijska funkcija, ako se testira na skupu uzoraka "sličnom" skupu za učenje, imati pogrešku testiranja blisku pogrešci za učenje. Stoga je algoritam učenja temeljen na robusnoj optimizaciji (npr. Lasso) samim time robustan budući da u osnovi smanjuje gornju granicu pogrešaka testiranja na skupovima uzoraka koji su "slični" skupu za učenje. S druge strane, "stabilnost", kako formalno definiramo u nastavku, odnosi se na svojstvo algoritma da će, ako se trenira na "malo drugačijim" skupovima uzoraka, imati "slične" izlazne funkcije. Stoga, u osnovi, algoritam može biti robustan, ali nestabilan, jer, iako može ispisati dvije značajno različite regresijske funkcije s dva slična skupa uzoraka, pogreška, ako se testira na drugom skupu, ne mora biti mnogo veća. Ovaj odjeljak pokazuje da Lasso spada upravo u tu kategoriju.

Najprije se prisjetimo definicije uniformne stabilnosti. Ugrubo, algoritam je stabilan ako izlazna funkcija nema jaku ovisnost ni o jednom danom skupu za učenje, tj. izlazna funkcija se neznatno mijenja ako se ukloni bilo koji skup za učenje.

Da budemo precizniji, neka $\mathcal{X}$ označava prostor (označenih) primjeraka (obično će to biti kompaktni podskup od $\mathbb{R}^{m+1}$) tako da $S \in \mathcal{X}^n$ označava kolekciju od n označenih primjeraka skupa za učenje. Neka $\mathbb{L}$ označava algoritam učenja, a za $S \in \mathcal{X}^n$, neka $\mathbb{L}_S$ označava izlaz algoritma učenja (tj. regresijsku funkciju koja je naučena iz podataka za učenje). Zatim s obzirom na funkciju gubitka l i označenu točku $s = (\mathbf{z}, b) \in \mathcal{X}$, pustimo

da $l(\mathbb{L}_S, s)$ označava gubitak algoritma koji je uvježban na skupu S, na podatkovnoj točki s. Stoga bismo za kvadrat gubitaka imali $l(\mathbb{L}_S, s) = \|\mathbb{L}_S(\mathbf{z}) - b\|_2$.

Definicija 2.6.1. *Algoritam $\mathbb{L}$ je uniformno stabilan s granicom stabilnosti β_n s obzirom na funkciju gubitka l ako vrijedi sljedeće:*

$$(\forall S \in \mathcal{X}^n)(\forall i \in \{1, \cdots, n\}); \|l(\mathbb{L}_S, \cdot) - l(\mathbb{L}_{S^{\setminus i}}, \cdot)\|_\infty \leq \beta_n.$$

Ovdje $\mathbb{L}_{S^{\setminus i}}$ označava naučeno rješenje s i-tim uzorkom uklonjenim iz S.

Mnogi algoritmi učenja imaju razumnu stabilnost kao na primjer Tikhonovljeva regularizirana regresija. Nasuprot tome, u ovom odjeljku pokazujemo da ne samo da je stabilnost (u gore definiranom smislu) Lasso regularizacije mnogo gora od stabilnosti ℓ_2-regularizirane regresije, nego je zapravo njena stabilnost, u preciznom smislu, najgora moguća. U tu svrhu, definiramo pojam trivijalne granice kao najgoru moguću pogrešku koju algoritam za učenje može imati, s obzirom na proizvoljan skup za učenje i uzorak za testiranje označen nulom.

Definicija 2.6.2. *Dana je funkcija gubitka l, podskup iz kojeg možemo izvući m označenih točaka, $\mathcal{Z} \subseteq \mathbb{R}^{n\times(m+1)}$ i podskup za jednu neoznačenu točku, $\mathcal{X} \subseteq \mathbb{R}^m$, trivijalna granica za algoritam učenja $\mathbb{L}$ u odnosu na $\mathcal{Z}$ i $\mathcal{X}$ je*

$$\mathfrak{b}(\mathbb{L}, \mathcal{Z}, \mathcal{X}) \coloneqq \max_{S\in\mathcal{Z}, \mathbf{z}\in\mathcal{X}} l(\mathbb{L}_S, (\mathbf{z}, 0)).$$

No, trivijalna se granica ne smanjuje kako se broj uzoraka povećava, budući da će ponovljenim odabirom najlošijeg uzorka algoritam dati isto rješenje. Sada pokazujemo da uniformna granica stabilnosti Lasso-a ne može biti bolja od njegove trivijalne granice s prepolovljenim brojem značajki. Dokaz je konstruktivan: dajemo primjer gdje će dodavanjem ili uklanjanjem jednog uzorka za treniranje Lasso dati značajno različite regresijske funkcije. Ugrubo, nestabilnost Lasso regularizacije uzrokovana je činjenicom da njegova ciljna funkcija koja se minimizira nije glatka.

Teorem 2.6.3. *Neka je $\hat{\mathcal{Z}} \subseteq \mathbb{R}^{n\times(2m+1)}$ domena skupa uzoraka i $\hat{\mathcal{X}} \subseteq \mathbb{R}^{2m}$ domena novog opažanja, tako da*

$$(\mathbf{b}, A) \in \mathcal{Z} \Longrightarrow (\mathbf{b}, A, A) \in \hat{\mathcal{Z}}$$
$$(\mathbf{z}^\top) \in \mathcal{X} \Longrightarrow (\mathbf{z}^\top, \mathbf{z}^\top) \in \hat{\mathcal{X}}.$$

Tada je uniformna granica stabilnosti Lasso regularizacije odozdo ograničena s $\mathfrak{b}(\text{Lasso}, \mathcal{Z}, \mathcal{X})$.

Dokaz. Neka su $(\mathbf{b}^*, A^*)$ i $(0, \mathbf{z}^{*\top})$ skup uzoraka i novo opažanje tako da zajedno postižu $\mathfrak{b}(\text{Lasso}, \mathcal{Z}, \mathcal{X})$ i neka je x^* optimalno rješenje Lasso-a u odnosu na $(\mathbf{b}^*, A^*)$.
Razmotrimo sljedeći uzorak

$$\begin{pmatrix} \mathbf{b}^* & A^* & A^* \\ 0 & \mathbf{0}^\top & \mathbf{z}^{*\top} \end{pmatrix}.$$

Uočimo da je $(\mathbf{x}^{*\top}, \mathbf{0}^\top)^\top$ optimalno rješenje Lasso-a u odnosu na taj uzorak. Uklonimo zadnji primjerak iz skupa za učenje. Primijetimo sada da je $(\mathbf{0}^\top, \mathbf{x}^{*\top})^\top$ optimalno rješenje za taj novi skup. Korištenjem posljednjeg uzorka kao opažanja testiranja, rješenje s obzirom na potpuni skup uzoraka ima nultu cijenu, dok rješenje izostavljenog skupa uzoraka ima trošak $\mathfrak{b}$ (Lasso, $\mathcal{Z}, \mathcal{X}$). Dakle, dokazali smo tvrdnju teorema. □

Napominjemo da primjer u dokazu ne bi funkcionirao za ℓ_2 regularizaciju, jednostavno zato što ℓ_2 regularizacija raspoređuje težinu između identičnih značajki kako bi se postigla strogo manja kazna regularizacije, tj. $(\mathbf{x}^*/2, \mathbf{x}^*/2)$ je bolje rješenje i od $(\mathbf{x}^*, 0)$ i od $(0, \mathbf{x}^*)$. Doista, sposobnost identificiranja redundantnih značajki (tj. odabira samo jedne između identičnih značajki) dovodi do nestabilnosti Lasso-a i mnogih drugih rijetkih algoritama.

Bibliografija

[1] Huan Xu, Constantine Caramanis i Shie Mannor, *Robustness and Regularization of Support Vector Machines*, Journal of machine learning research **10** (2009).

[2] Bertsimas Dimitris, David B. Brown i Constantine Caramanis, *Theory and applications of robust optimization*, SIAM Review **53** (2011), 464–501.

[3] Anthony L. Peressini, Francis E. Sullivan i Jerry J. Uhl, *The mathematics of nonlinear programming*, Springer, New York, 1988.

[4] Huan Xu, Constantine Caramanis i Shie Mannor, *Robust Regression and Lasso*, Advances in Neural Information Processing Systems (D. Koller, D. Schuurmans, Y. Bengio i L. Bottou, ur.), Curran Associates Inc., New York, 2008., str. 1801–1808.

[5] Constantine Caramanis, Shie Mannor i Huan Xu, *Robust Optimization in Machine Learning*, Optimization for Machine Learning (Stephen J. Wright Suvrit Sra, Sebastian Nowozin, ur.), MIT Press, London, 2012, str. 369–402.

Sažetak

U ovom radu prikazali smo primjene nekih tehnika robusne optimizacije u strojnom učenju. Robusna optimizacija važan je dio optimizacije koji se bavi nesigurnošću u podacima optimizacijskih problema. Kako se u današnje vrijeme strojno učenje često susreće s nesigurnošću, robusna optimizacija tu ima sve veću ulogu. Promatrana je veza između robusnosti i regulariziranog stroja potpornih vektora, točnije, pokazali smo da je standardni regularizirani stroj potpornih vektora posebni slučaj robusne optimizacije. Zatim je uvedena robusna regresija s pogreškom najmanjih kvadrata te je promatran slučaj gdje su značajke izložene smetnjama, to jest nesigurnosti. Osigurana je interpretacija Lasso algoritma s robusne perspektive, a na temelju te robusne interpretacije istražena su svojstva rijetkosti i konzistentnosti. Osim toga, predstavljen je rezultat koji nam govori da su rijetkost i stabilnost u kontradikciji, to jest da se ne mogu postići simultano.

Summary

In this paper, we presented some robust optimization techniques in machine learning. Robust optimization is an important part of optimization that deals with uncertainty in the data of optimization problems. As today's machine learning is often faced with uncertainty, robust optimization plays an increasingly important role. The connection between robustness and regularized support vector machine was observed, more precisely, we showed that the standard regularized support vector machine is a special case of robust optimization. Robust regression with least squares error was introduced and the case where the features are exposed to disturbances, that is, uncertainties, was observed. An interpretation of the Lasso algorithm from a robust perspective is provided, and on the basis of this robust interpretation, the properties of sparsity and consistency are investigated. In addition, a result is presented that tells us that sparsity and stability are in contradiction, that is, they cannot be achieved simultaneously.

Životopis

Rođena sam 22. studenog 1996. godine u Koprivnici. Završila sam Osnovnu školu Kalnik i nakon toga upisala Gimnaziju Ivana Zakmardija Dijankovečkoga Križevci. Srednju školu završila sam 2015. godine i iste godine upisala sam preddiplomski sveučilišni studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Preddiplomski studij završila sam 2020. godine i iste godine upisala sam diplomski studij Računarstvo i matematika na istom fakultetu.