

Strojno učenje – domaća zadaća 5

UNIZG FER, ak. god. 2016./2017.

Zadano: 15. 11. 2016. Rok: 18. 11. 2016.

Napomena: Zadatke možete rješavati samostalno ili u grupi. Ako zadatke rješavate u grupi, pobrinite se da svi članovi grupe pridonose rješenju i da ga naposlijetu svi razumiju. Po potrebi konzultirajte sve dostupne izvore informacija. Rješenja zadataka ponesite na iduće auditorne vježbe. Zabilježite sve nejasnoće i nedoumice, kako bismo ih prodiskutirali.

1. [Svrha: Razumjeti izvod modela stroja potpornih vektora.]

- (a) Definirajte, korak po korak, problem maksimalne margine (tvrdna marge).
- (b) Definirajte, korak po korak, dualni problem maksimalne margine te pripadne KKT-uvjetne kojih vrijede u točci rješenja.
- (c) Koje su prednosti formulacije problema kao dualnoga optimizacijskog problema?
- (d) Napišite primarnu i dualnu formulaciju modela SVM.
- (e) Zašto kažemo da je SVM, uz dualnu formulaciju problema, neparametarski model? Koja je prednost takvog modela u smislu računalne učinkovitosti? Dolazi li taj prednost do izražaja kod treniranja ili kod uporabe modela (predikcije)?

2. [Svrha: Isprobati izračuna modela potpornih vektora na konkretnom numeričkom primjeru i tako bolje razumjeti formule. Razumjeti povezanost primarne i dualne formulacije problema.] Raspolažemo sljedećim primjerima za učenje:

$$\mathcal{D} = \{(\mathbf{x}^{(i)}, y^{(i)})\}_i = \{((0, 0), -1), ((2, 4), -1), ((4, 2), -1), ((6, 4), +1), ((6, 8), +1), ((8, 8), +1)\}$$

- (a) Skicirajte primjere u ulaznom prostoru \mathbb{R}^2 i granicu maksimalne margine za te primjere. Napišite izraz za linearni model $h(\mathbf{x})$ koji odgovara toj granici.
- (b) Odredite širinu marge.
- (c) U ovom slučaju potporni vektori su $\mathbf{x}^{(3)} = (4, 2)$ i $\mathbf{x}^{(4)} = (6, 4)$. Odredite vektor Lagrangeovih koeficijenata α temeljem izraza (7.5) iz skripte.
- (d) Upoznajte se s formulom (7.8) iz skripte (taj dio smo na predavanjima preškocili) te izračunajte pomak w_0 .
- (e) Odredite klasifikaciju novog primjera $\mathbf{x}^{(7)} = (5, 6)$ temeljem dualne reprezentacije granice.

3. [Svrha: Razumjeti potrebu za mekom marginom. Znati izvesti problem meke marge SVM-a preko Lagrangeove dualnosti.]

- (a) Objasnite motivaciju za uvođenje meke marge. Skicirajte primjer prenaučenosti uslijed meke marge, i to za linearno odvojiv i linearno neodvojiv slučaj.

- (b) Formulirajte problem optimizacije meke margine.
 - (c) Definirajte dualni kvadratni problem za meku marginu.
 - (d) Krenuvši od KKT-uvjeta, dokažite da potporni vektori za koje vrijedi $\alpha_i \leq C$ leže na margini, a vektori za koje $\alpha_i = C$ unutar margine.
4. [Svrha: Znati izvesti formulaciju algoritma SVM preko gubitka zglobnice. Razumjeti funkciju pogreške SVM-a.]
- (a) Krenuvši od problema meke margine, izvedite gubitak zglobnice.
 - (b) Prepostavite da je ispravna klasifikacija primjera $\mathbf{x}^{(7)} = (5, 6)$ iz zadatka 2 negativna. Koliko iznosi gubitak koji primjer $\mathbf{x}^{(7)}$ nanosi modelu treniranom u zadatku 2?
 - (c) Skicirajte pogrešku učenja i pogrešku ispitivanja kao funkciju od C . Kojem području odgovara prenaučenost a kojem podnaučenost?
 - (d) Pokušajte odgovoriti: zašto SVM rezultira rijetkim modelima, unatoč tome što zapravo koristi L2-regularizaciju, za koju je poznato da ne rezultira rijetkim modelima? (Pomoć: usporedite gubitak zglobnice i gubitak logističke regresije.)

5 DOMAĆA ZADACA

1 DEF, KORAK PO KORAK, PROBLEM MAKSIMALNE (VRDE) MARGINE.

a) MODEL: $h(x) = \vec{w}^T \phi(x) + w_0 \Rightarrow$ linearan model bez aktivacijske funkcije
OZNAKE PR. ZA UČENJE: $y \in \{-1, 1\}$ (radi jednostavnosti).

PREDIKCIJA ZA NOVI PRIMJER X : $y = \text{sgn}(h(x))$
↳ (PREDIKCIJA KLASE)

⇒ Pretpostavimo da su primjeri \mathcal{D} linearno odvojivi:

$$\hookrightarrow \text{Postoje } \vec{w} \text{ i } w_0 \text{ takvi da: } \begin{cases} h(x^{(i)}) \geq 0 \text{ za } y^{(i)} = +1 \\ h(x^{(i)}) < 0 \text{ za } y^{(i)} = -1 \end{cases} \quad \begin{array}{l} h(x^{(i)}) \geq 0 \\ y^{(i)} h(x^{(i)}) \geq 0 \end{array}$$

↳ Nas zanima rješenje MAKSIMALNE MARGINE, odnosno NAJVEĆA UDALJENOST HYPERRAVNINE OD NAJBUDŽEG PRIMJERA.

→ PREDSTAVLJENA UDALJENOST PR. OD HYPERPLANE = $d = \frac{|h(x)|}{\|\vec{w}\|}$

→ Nas zanimašo samo rješenja kod kojih su sve točke ispravno klasificirane. U tomu slučaju udaljenost od hyperplane je jednaka:

$$d = \frac{|h(x)|}{\|\vec{w}\|} = \frac{|y^{(i)} h(x^{(i)})|}{\|\vec{w}\|} = \frac{|y^{(i)} (\vec{w}^T \phi(x^{(i)}) + w_0)|}{\|\vec{w}\|} \rightarrow |y^{(i)} (\vec{w}^T \phi(x^{(i)}) + w_0)| \geq d \geq 0 !$$

⇒ MARGINA - UDALJENOST DO NAJBUDŽEG PRIMJERA! (≥ 0)

$$\hookrightarrow d_{\text{marg}} = \frac{1}{\|\vec{w}\|} \min_i \{ |y^{(i)} (\vec{w}^T \phi(x^{(i)}) + w_0)| \}$$

↳ Nas zanimašo vrijednosti parametara \vec{w} i w_0 za koje će margin biti max!. Odnosno tu udaljenost želimo maksimalizirati.
Ako su primjeri \mathcal{D} linearno odvojivi tad postoji samo jedna taluka margini:

$$\underset{\vec{w}, w_0}{\text{argmax}} \left\{ \frac{1}{\|\vec{w}\|} \min_i \{ |y^{(i)} (\vec{w}^T \phi(x^{(i)}) + w_0)| \} \right\}$$

→ Zbog pojednostavljenja problema pretpostavimo da za primjer koji je najbliži margini vrijedi $|y^{(i)} (\vec{w}^T \phi(x^{(i)}) + w_0)| = 1$. Uvrstavajući u gornji izraz pišemo:

$$\underset{\vec{w}, w_0}{\text{argmax}} \left\{ \frac{1}{\|\vec{w}\|} \right\}, \text{ uz ograničenje } y^{(i)} (\vec{w}^T \phi(x^{(i)}) + w_0) \geq 1$$

ekvivalentno:

$$\underset{\vec{w}, w_0}{\text{argmax}} \left\{ \frac{1}{2} \|\vec{w}\|^2 \right\}$$

⇒ ŠIRINA MAX MARGINE

$$\frac{2}{\|\vec{w}\|}$$

b) DEF KORAK PO KORAK DUALNI PROBLEM MAX MARGINE JE PRIPADNEK K KUTIJE.

Problem je a) postavljatice možemo jesti uodjicem LAGRANGEOVU MULTPLIKATORA.

⇒ LAGRANGEVA FUNKCIJA
(PRIMARNI PROBLEM)

$$L(\vec{w}, w_0, \vec{\lambda}) = \frac{1}{2} \|\vec{w}\|^2 - \sum_{i=1}^n \lambda_i \{y^{(i)}(\vec{w}^\top \Phi(x^{(i)}) + w_0) - 1\}$$

↳ $\vec{\lambda} = (\lambda_1, \dots, \lambda_N)$ → vektor Lagrangeovih množplikatora

→ PRELAZAK U DUALNI PROBLEM

$$\frac{\partial L}{\partial \vec{w}} = \emptyset$$

$$\frac{\partial L}{\partial w_0} = \emptyset$$

$$\frac{\partial L}{\partial \vec{w}} = \frac{1}{2} (2\vec{w}^\top) - \sum_{i=1}^n \lambda_i \{y^{(i)} \Phi^\top(x^{(i)})\} = \emptyset \quad \vec{w}^\top = \sum_{i=1}^n \lambda_i y^{(i)} \Phi^\top(x^{(i)})$$

$$\frac{\partial L}{\partial w_0} = - \sum_{i=1}^n \lambda_i y^{(i)} = \emptyset$$

$$\sum_{i=0}^n \lambda_i y^{(i)} = \emptyset$$

$$\vec{w} = \sum_{i=1}^n \lambda_i y^{(i)} \Phi(x^{(i)})$$

w₀w

u L(\vec{w} , w₀, $\vec{\lambda}$)

$$\Rightarrow \tilde{L}(\vec{\lambda}) = \frac{1}{2} \|\vec{w}\|^2 - \sum_{i=1}^n \lambda_i \{y^{(i)}(\vec{w}^\top \Phi(x^{(i)}) + w_0) - 1\} = \\ = \frac{1}{2} \sum_{i=1}^n \lambda_i y^{(i)} \Phi^\top(x^{(i)}) \sum_{i=1}^n \lambda_i y^{(i)} \Phi(x^{(i)}) - \sum_{i=1}^n \lambda_i y^{(i)} \left(\sum_{i=1}^n \lambda_i y^{(i)} \Phi^\top(x^{(i)}) \Phi(x^{(i)}) + w_0 \right) - \sum_{i=1}^n \lambda_i y^{(i)} + \sum_{i=1}^n \lambda_i$$

$$\tilde{L}(\vec{\lambda}) = \sum_{i=1}^n \lambda_i - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \lambda_i \lambda_j y^{(i)} y^{(j)} \Phi^\top(x^{(i)}) \Phi(x^{(j)})$$

DUALNI PROBLEM ZATREBA MAXIMIZACIJP ABOV VZRAJA! MUZ KKT uvjeti:

⇒ i) DUALNI OPT.
PROBLEM

$$\tilde{L}(\vec{\lambda}) = \underset{\vec{\lambda}}{\operatorname{argmax}} \left\{ \sum_{i=1}^n \lambda_i - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \lambda_i \lambda_j y^{(i)} y^{(j)} \Phi^\top(x^{(i)}) \Phi(x^{(j)}) \right\}$$

ii) OGRANIČENJA
NA $\vec{\lambda}$

$$\lambda_i \geq 0 \quad i \quad \sum_{i=1}^n \lambda_i y^{(i)} = 0$$

iii) KKT

$$1) \lambda_i \geq 0 \quad 2) y^{(i)} \Phi^\top(x^{(i)}) - 1 \geq 0$$

$$3) \lambda_i (y^{(i)} \Phi^\top(x^{(i)}) - 1) = 0$$

Samo je ispunjeno za $\lambda_i = 0$ kada
 $y^{(i)} \Phi^\top(x^{(i)}) = 1$

Svi se vektori
zadovarjuju jer
ne učestvuju na
izlaznoj mjeri

LIN. KOMB. PONP. VEKTORA
DEFINIRA HYPERRAUNINU

SAMO PONP. VEKTORE
ZADOVALJAVU NAKON UČITVU MODELA!

C) PREDNOST FORMULACIJE PROBLEMA KAO DUALNOG OPTIMIZACIJSKOG PROBLEMA?

- Od $(n+1)$ primarnih varijabli problem smo sveli na N DUALNIH VAR.
(Smanjena računska složenost u slučaju većeg broja znacajki odnosno
broja primjera za učenje (npr. klasifikacija telista)).
- Moguće koristiti jednogog TRIKA! Ovo uogušci jidnostavno
prelikavanje u visokodimenzijski prostor znacajki.
- Moguće koristiti poseban optimizacijski postupak SMO, time smanjenu
računsku složenost s $O(n^3)$ na $O(N^2)$!

d) NAPISI PRIMARNU I DUALNU FORMULACIJU MODELA SVM

$$h(x) = \vec{w}^T \Phi(x) + w_0 = \sum_{i=1}^n \lambda_i y^{(i)} \Phi^T(x^{(i)}) \Phi(x) + w_0$$

PRIMARNA FORM.

DUALNA FORMULACIJA

↳ RACUNAMO SKAL. PRODUKT

PR. X USPOREDJUJEMO SA SUM
PR. $x^{(i)}$ je ŠUMA D

USPOREDJUJEMO KAKO JE
X SUCAN PR. $x^{(i)}$ U
PESTOBOZNIKU

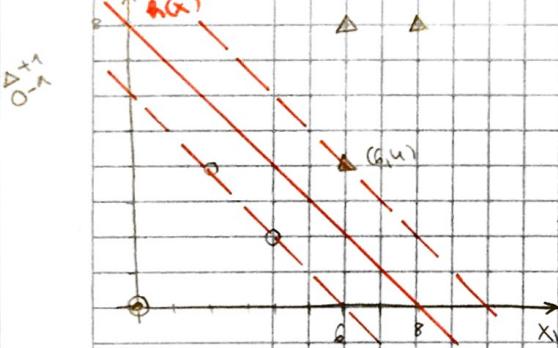
- e) ZASTO KAZEMO DA JE SUM NEPARAM MODEL? PREDNOST TAKVOG MODELA U SMISU RAC. UANKOVITOSTI?
DOLAZI U DA PREDNOST DO IZRAZAJA KOD NEONIKANJA ILI UPORABE

→ U dualnoj formulaciji, umjesto da poliranjujemo tezine \vec{w} , moramo polirati primere i njihove oznake. → EFEKTIVNO SMO DOBIVI NEPARAHETARSKI MODEL.
 $(x^{(i)}, y^{(i)})$ poliranjuje
↳ U dualnoj formulaciji broj parametara ovisi o broju primera.

→ PREDNOST: Obavljamo MANJE RAC. OPERACIJE → manje $t/*$ zalog upotrebe Kernela
→ Ta prednost dolazi do izraza kod PREDIKCIJE!

② $D = \{(x^{(i)}, y^{(i)})\}_{i=1}^7 = \{((0,0), -1), ((2,4), -1), ((4,2), -1), ((6,4), +1), ((6,8), +1), ((8,8), +1)\}$

a) SKICIRAJTE PR. U UL. PROSTORU R^2 I GRANICI MATE MARGINE ZA RE PR. NAPISI
IZRAT ZA $h(x)$ UNUTROŠOG MODELA koji ODGOVARA TOJ GRANICI.



HYPERRAVNINA $x_2 = -x_1 + 8 \Rightarrow x_2 + x_1 - 8 = 0$

$h(x)$ za točke na margini mora biti ± 1

$h(6,4) = 2 \neq 1 \rightarrow$ Treba podjeliti s 2!

$$h(x) = \frac{1}{2}(x_1 + x_2) - 4 \Rightarrow \vec{w} = \begin{bmatrix} -4 & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

$$\hookrightarrow h(x) = \underbrace{\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \end{bmatrix}}_{\vec{w}^T} \underbrace{\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}}_{\vec{x}} + [-4] \quad w_0$$

b) ŠIRINA MARGINE?

$$= \frac{2}{\|\vec{w}\|}$$

$$\text{gdje je } \|\vec{w}\| = \sqrt{0.5^2 + 0.5^2} = 2\sqrt{2}$$

$$\vec{w} = [0.5 \ 0.5]$$

c) PON. VEKTORI su $x^{(3)} = (4,2)$, $x^{(4)} = (6,4)$. $\vec{d} = ?$ → rešenjem (7.5)

$$\vec{w} = \sum_{i=1}^n \lambda_i y^{(i)} \Phi(x^{(i)})$$

$$\vec{w} = \lambda_3 y^{(3)} \Phi(x^{(3)}) + \lambda_4 y^{(4)} \Phi(x^{(4)})$$

$$\vec{w} = [0.5 \ 0.5]^T$$

$$\begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix} = -\lambda_3 \begin{bmatrix} 4 \\ 2 \end{bmatrix} + \lambda_4 \begin{bmatrix} 6 \\ 4 \end{bmatrix}$$

$$\Phi = \begin{bmatrix} 1 & 4 & 2 \\ 1 & 6 & 4 \end{bmatrix}$$

$$0.5 = -4\lambda_3 + 6\lambda_4$$

$$y = [-1 \ 1]^T$$

$$0.5 = -2\lambda_3 + 4\lambda_4$$

$$-0.5 = -8\lambda_3 + 6\lambda_4$$

$$-\frac{1}{2} = -2\lambda_3$$

$$\lambda_3 = 0.25$$

$$\hookrightarrow -\lambda_1 + \lambda_2 = 0$$

$$\lambda_1 = \lambda_2$$

$$\lambda_2 = 0.25$$

$$\lambda = [0.25 \ 0.25]$$

d) Izr. pomak w_0 i upoznaј se s (7.8)

$$w_0 = \frac{1}{|S|} \sum_{i \in S} \left(y^{(i)} - \sum_{j \in S} \alpha_j y^{(j)} \Phi^T(x^{(j)}) \Phi(x^{(i)}) \right)$$

$$\alpha = [0.25 \ 0.25]$$

$$y = [-1 \ 1]$$

$$\Phi = \begin{bmatrix} 1 & 1 \\ 4 & 2 \\ 6 & 4 \end{bmatrix}$$

$$\Phi^3 = [4 \ 2] \quad \Phi^4 = [6 \ 4]$$

S - skup indeksa potpornih vektora

$$w_0 = \frac{1}{2} \left(y^{(3)} - \alpha_3 y^{(3)} \Phi^T(x^{(3)}) \Phi(x^{(3)}) - \alpha_4 y^{(4)} \Phi^T(x^{(3)}) \Phi(x^{(4)}) + y^{(4)} - \alpha_3 y^{(3)} \Phi^T(x^{(4)}) \Phi(x^{(3)}) - \alpha_4 y^{(4)} \Phi^T(x^{(4)}) \Phi(x^{(4)}) \right) = \frac{1}{2} (-1 + 5 - 8 + 1 + 8 - 13) \Rightarrow w_0 = -4$$

e) $x^{(7)} = (5, 6)$ KLASIF? \rightarrow TEMEĆEM DUALNE REPREZENTACIJE GRANICE

$$h(x) = w^T \Phi(x) + w_0 = \sum_{i \in S} \alpha_i y^{(i)} \Phi^T(x^{(i)}) \Phi(x) + w_0$$

$$h(x^{(7)}) = \alpha_3 y^{(3)} \Phi^T(x^{(3)}) \Phi(x^{(7)}) + \alpha_4 y^{(4)} \Phi^T(x^{(4)}) \Phi(x^{(7)}) + w_0$$

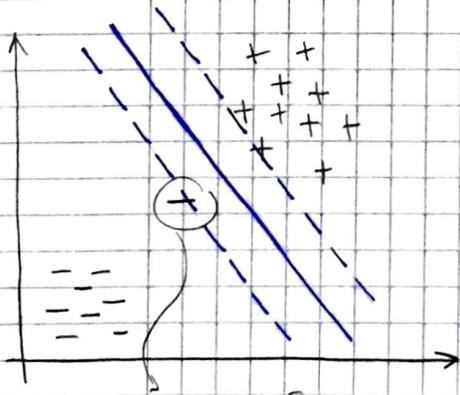
$$= (0.25)(-1)[4 \ 2][5] + (0.25)(1)[6 \ 4][5] - 4$$

$$= -8 + 13.5 - 4 = 1.5 \quad h(x^{(7)}) = 1.5 \Rightarrow y(x^{(7)}) = +1$$

③ a) Motivacija za upotrebu NEKE MARGINE? SKICAJ PR. PRAVAKOČNOSTI USUJED MJEKE MARG.) ZA LIN. ODV. I LIN. NEODV. SL.

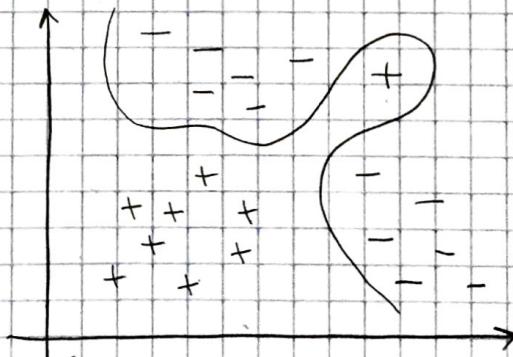
- SUKLADNO COLEKTOVI TCM puno je vjerovatnije da će problem biti linearno neodgovor nego da će biti linearno odgovor.
 - Ne zelimo da model bude svihne linearan jer bi to moglo dovesti do pravakonosti, odnosno do prilagodbe formu u podacima.
 - Ne zelimo da model itčubi svojstvo GENERALIZACIJE, stoga proširujemo prethodni model tako da on dozvoljava da u njemu primjeri ipak budu pogrešno klasificirani \Rightarrow MJEKA MARGINA!
- \Rightarrow Kod mjeke marge dozvoljavamo da pr. budu na pogrešnoj strani granice, ali to kožnjavamo tim više što se pr. nalaze dublje na pogrešnoj strani granice. !

i) LIN. ODOVNI PRIMJERI



OUTIER \rightarrow SUM
SUŽROKUJE NEPOKREBNO USKU
MARGINU! MJEKA MARGINA BI
BILA BUŽE MINUSIMA, A
OUTIER BI KAŽNILA

ii) LIN. NEODGOJVU SKICAJ



\Rightarrow MODEL PREVIŠE SLOŽEN!
PRAVAKON, PREVIŠE SMO
SE PRILAGODI LI PODACIMA
(I PUMI)

b) FORMULIRAJ PROBL. OPTIMIZACIJE MEKE MARGINE

$$\underset{\vec{w}, w_0}{\operatorname{argmin}} \left\{ \frac{1}{2} \|\vec{w}\|^2 + C \sum_{i=1}^n \xi_i \right\} \quad \text{už. } \xi_i \geq 0 \text{ i } y^{(i)}(\vec{w}^\top \Phi(x^{(i)}) + w_0) \geq 1 - \xi_i$$

$\hookrightarrow C = 1/\lambda > 0 \rightarrow$ određuje kompromis između veličine marge i ukupne kazne. $C \uparrow \text{kazna} \uparrow \text{složenost modela} \uparrow$

c) DEF. DUALNI KUADRATNI PROBL. ZA MEGLE MARGINU

$$\underset{\lambda}{\operatorname{argmax}} \sum_{i=1}^n \lambda_i - \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \lambda_i \lambda_j y^{(i)} y^{(j)} \Phi^\top(x^{(i)}) \Phi(x^{(j)})$$

\hookrightarrow isto kao za tvar, ali se razlikuju ograničenja:

- i) $0 \leq \lambda_i \leq C$
- ii) $\sum_{i=1}^n \lambda_i y^{(i)} = 0$ $(\in \mathbb{R}^{1 \times n})$

d) NE UZMI U ISPLIT

a) IZVOD ZA GUBITAK ZAKONICE KROVNOŠĆI OD PROBL. MEKE MARGINE

\rightarrow za pr. koji su na ispravnoj strani marge vrijedi: $y^{(i)} f_h(x^{(i)}) \geq 1$
Ove pr. ne kažnjavamo!

\rightarrow pr. koji su na poogr. str. marge ili unutar međužupljivosti s $\xi_i = |y^{(i)} - f_h(x^{(i)})|$ jednako = $1 - y^{(i)} f_h(x^{(i)})$

\hookrightarrow za $y = +1$ kažnjavamo pr. zato što $f_h(x) \leq 1$
 $y = -1$ u - $f_h(x) \geq 1$

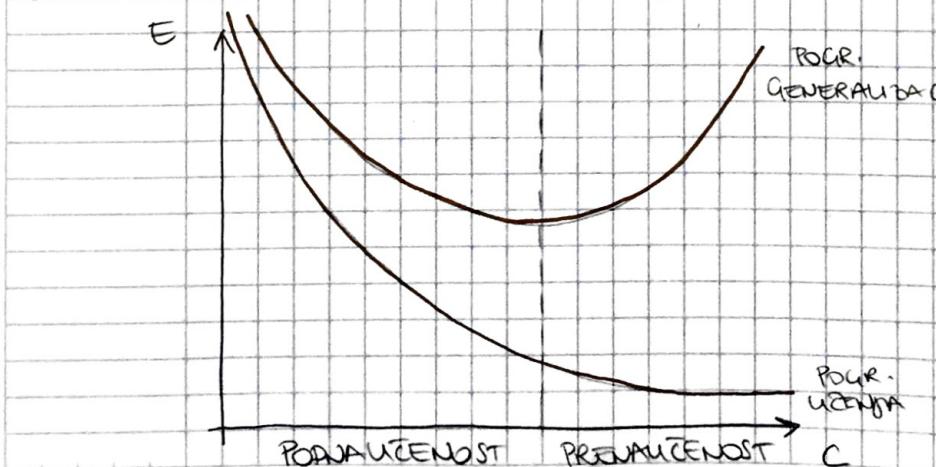
PREMA TOJUE, taj gubitak je

$$L(f_h(x), y) = \max(0, 1 - y f_h(x))$$

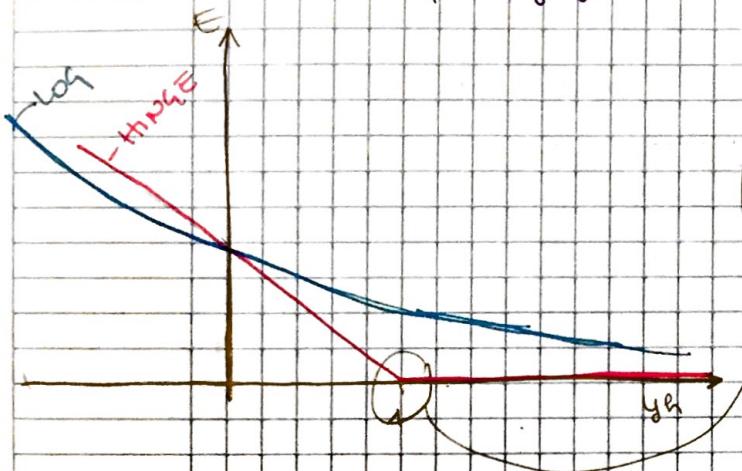
b) $x^{(1)} = (5, 6)$, $y = -1$ (aneš kao u prethodnom zad.). GUBITAK koji x^1 daje

$$y(x^{(1)}) = -1 \quad f_h(x^{(1)}) = 1.5 \quad L(f_h(x), y) = \max(0, 1 - (-1)(1.5)) = \underline{\underline{2.5}}$$

c) NACRTAN POGR. UCENJA / GEN. KAO FU (a. OZNACI PRENUC / PODNUC.)



a) ZASTO SUM REGULIRAN RYTHM MODELIMA UNATOČ TOGU ŽTO ZAPRVAO
KORISTI L2-REG, ZA KOJU JE POZNATO DA NE REGULIRAJE RJ. MOD?



↳ nika vidimo kako je za opravno klasifikaciju primjere funkcija zglobne jedinice ϕ , s obzirom da je vise rezina pritegnuta na ϕ rezultirajući nestim modelima.

U drugu ruku imamo log. reg. kod kojeg i opravno klasifikaciju prati najavajuci, stoga iako greska teži u ϕ , ona neće nikada biti jedinica ϕ , te stoga neće rezultirati nestim mod.