

## 2. Osnovni koncepti

Strojno učenje 1, UNIZG FER, ak. god. 2021./2022.

Jan Šnajder, natuknice s predavanja, v1.6

### 1 Primjena algoritma strojnog učenja

1. Priprema i analiza podataka
2. Opcionalno: Označavanje podataka za učenje i ispitivanje
3. Ekstrakcija značajki
4. Opcionalno: Redukcija dimenzionalnosti
5. **Odabir modela**
6. **Učenje modela**
7. **Vrednovanje modela**
8. Dijagnostika i ispravljanje
9. Instalacija

### 2 Primjeri, hipoteza, model

- Primjer je **vektor značajki**:  $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$
- $\mathcal{X}$  je **ulazni prostor (prostor primjera)**;  $\mathcal{Y}$  je skup oznaka
- Skup označenih primjera:  $\mathcal{D} = \{(\mathbf{x}^{(i)}, y^{(i)})\}_{i=1}^N \subseteq \mathcal{X} \times \mathcal{Y}$

	$x_1$	$x_2$	$\dots$	$x_n$	$\mathbf{y}$
$\mathbf{x}^{(1)} =$	$x_1^{(1)}$	$x_2^{(1)}$	$\dots$	$x_n^{(1)}$	$y^{(1)}$
$\mathbf{x}^{(2)} =$	$x_1^{(2)}$	$x_2^{(2)}$	$\dots$	$x_n^{(2)}$	$y^{(2)}$
	$\vdots$				
$\mathbf{x}^{(N)} =$	$x_1^{(N)}$	$x_2^{(N)}$	$\dots$	$x_n^{(N)}$	$y^{(N)}$

- **Hipoteza** – funkcija koja primjerima dodjeljuje oznake:  $h : \mathcal{X} \rightarrow \mathcal{Y}$
- **Binarna klasifikacija**:  $h : \mathcal{X} \rightarrow \{0, 1\}$

- Hipoteza je definirana do na parametre  $\theta$ : pišemo  $h(\mathbf{x}; \theta)$ 
  - Regresija u  $\mathcal{X} = \mathbb{R}$ :  $h(x; \theta_0, \theta_1) = \theta_1 x + \theta_0$
  - Klasifikacija pravcem u  $\mathcal{X} = \mathbb{R}^2$ :  $h(x_1, x_2; \theta_0, \theta_1, \theta_2) = \mathbf{1}\{\theta_1 x_1 + \theta_2 x_2 + \theta_0 \geq 0\}$
- gdje  $\mathbf{1}\{P\} = \begin{cases} 1 & \text{ako } P \equiv \top \\ 0 & \text{inače} \end{cases}$
- **Model** – skup hipoteza parametriziranih s  $\theta$ :  $\mathcal{H} = \{h(\mathbf{x}; \theta)\}_\theta$
- **Učenje (treniranje) modela** – pretraživanje skupa  $\mathcal{H}$  za najboljom hipotezom

### 3 Empirijska pogreška i funkcija gubitka

- **Empirijska pogreška**  $E(h|\mathcal{D})$  – iskazuje netočnost hipoteze  $h$  na skupu podataka  $\mathcal{D}$ 
  - Pogreška klasifikacije:  $E(h|\mathcal{D}) = \frac{1}{N} \sum_{i=1}^N \mathbf{1}\{h(\mathbf{x})^{(i)} \neq y^{(i)}\}$
- **Funkcija gubitka** (*loss function*)  $L(y, h(\mathbf{x}))$  – mjeri pogrešku na jednom primjeru
  - **Gubitak nula-jedan** (*zero-one loss*):  $L(y, h(\mathbf{x})) = \mathbf{1}\{h(\mathbf{x})^{(i)} \neq y^{(i)}\}$
- Empirijska pogreška je **očekivana vrijednost** funkcije gubitka na skupu  $\mathcal{D}$

### 4 Tri komponente algoritma strojnog učenja

1. **Model**:  $\mathcal{H} = \{h(\mathbf{x}; \theta)\}_\theta$
2. **Funkcija pogreške**:  $E(h|\mathcal{D})$  odnosno  $E(\theta|\mathcal{D})$
3. **Optimizacijski postupak** koji minimizira empirijsku pogrešku:

$$h^* = \operatorname{argmin}_{h \in \mathcal{H}} E(h|\mathcal{D})$$

odnosno:

$$\theta^* = \operatorname{argmin}_{\theta} E(\theta|\mathcal{D})$$

### 5 Složenost modela

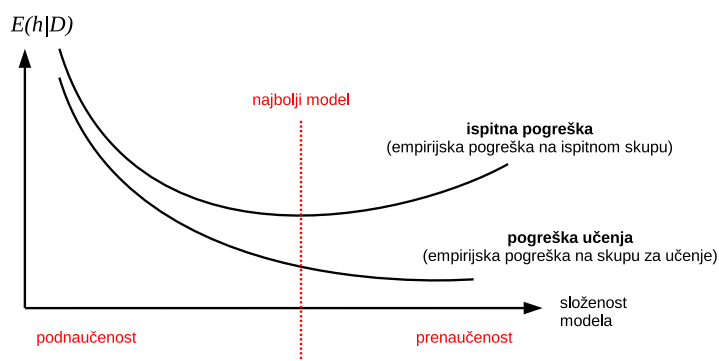
- U idealnom slučaju,  $E(h|\mathcal{D}) = 0$
- Ako  $\forall h \in \mathcal{H}. E(h|\mathcal{D}) > 0$ , onda model nije dovoljne **složenosti (kapaciteta)**
- **Šum** – neželjena anomalija u podacima
- Uzroci: nepreciznost, pogreške u označavanju, nedostajuće značajke, subjektivnost
- Posljedica šuma: granica između klasa je nepotrebno složena
- Presložen model previše se prilagođava šumu (uči šum)

## 6 Odabir modela

- Odabir modela iz **familije modela**  $\{\mathcal{H}_1, \mathcal{H}_2, \dots, \mathcal{H}_k\}$
- Složenost modela određena je **hiperparametrima** (npr. stupanj nelinearnosti)
- **Odabir modela = optimizacija hiperparametara**
- Preferiramo jednostavnije modele jer bolje **generaliziraju**, lakše se uče i tumače
- **Podnaučenost** –  $\mathcal{H}$  je prejednostavan u odnosu na stvarnu funkciju
- **Prenaučenost** –  $\mathcal{H}$  je presložen u odnosu na stvarnu funkciju
- Prenaučena hipoteza nije točna na neviđenim primjerima  $\Rightarrow$  loša generalizacija

## 7 Unakrsna provjera

- Ideja: dio primjera iz označenog skupa koristiti kao “neviđene” primjere
- Disjunktna podjela skupa na **skup za učenje** i **skup za ispitivanje**:  $\mathcal{D} = \mathcal{D}_{\text{train}} \cup \mathcal{D}_{\text{test}}$
- **Pogreška učenja** (*train error*):  $E(h|\mathcal{D}_{\text{train}})$
- **Ispitna pogreška** (*test error*):  $E(h|\mathcal{D}_{\text{test}})$
- $E(h|\mathcal{D}_{\text{train}})$  pada sa složenošću modela,  $E(h|\mathcal{D}_{\text{test}})$  tipično prvo opada a zatim raste
- Skica: pogreška učenja i ispitna pogreška kao funkcije složenosti modela



- Optimalan model je onaj koji minimizira  $E(h|\mathcal{D}_{\text{test}})$