Nadzirani pristupi za procjenu nesigurnosti predikcija dubokih modela

Ivan Grubišić Voditelj: Siniša Šegvić

Fakultet elektrotehnike i računarstva

- 1 Procjena nesigurnosti kod dubokih modela
- 2 Izražavanje nesigurnosti predikcije
- **3** Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita
- ♠ Eksperimenti: procjena nesigurnosti kod semantičke segmentacije pomoću dropouta
- **6** Eksperimenti: prepoznavanje izvanrazdiobnih primjera
- 6 Zaključak

- 1 Procjena nesigurnosti kod dubokih modela
- 2 Izražavanje nesigurnosti predikcije
- 9 Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita
- Eksperimenti: procjena nesigurnosti kod semantičke segmentacije pomoću dropouta
- **6** Eksperimenti: prepoznavanje izvanrazdiobnih primjera
- Zaključak

Procjena nesigurnosti kod dubokih modela

- Trenutno najuspješniji modeli često pokazuju preveliku sigurnost u
 predikcije kod izvanrazdiobnih i krivo klasificiranih primjera
 [10, 5, 6], a mogu se i pronalaziti neprijateljski primjeri [14, 4].
- Neki oblici strojnog učenja, posebno podržano i aktivno učenje mogu imati koristi od razlikovanja je li uzrok nesigurnosti višeznačnost podataka ili neznanje, tj. nesigurnost u parametre.
- Složeni modeli se sve više koriste u sustavima koji donose odluke o kojima ovise sigurnost i zdravlje ljudi, pa trebaju biti sposobni pouzdano procijeniti nesigurnost/rizik.

Procjena nesigurnosti kod dubokih modela

- Nesigurnost možemo podijeliti [1] na:
 - aleatornu nesigurnost (lat. aleator, kockar) nesigurnost koja dolazi
 od višeznačnosti podataka i ne može se smanjiti zbog nedeterminizma
 procesa koji generira podatke,
 - epistemičku nesigurnost (grč. epistēmē, znanje) ili nesigurnost modela – nesigurnost kojoj je uzrok nedostatak znanja i može se smanjiti uz više podataka.
- Granica između aleatorne i epistemičke nesigurnosti nije uvijek jasna.
- Epistemička nesigurnost predikcije proizlazi iz nesigurnosti u parametre, koju izražava aposteriorna razdioba parametara – potrebno je bayesovsko zaključivanje o parametrima modela.

- 1 Procjena nesigurnosti kod dubokih modela
- 2 Izražavanje nesigurnosti predikcije
- 3 Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita
- Eksperimenti: procjena nesigurnosti kod semantičke segmentacije pomoću dropouta
- **6** Eksperimenti: prepoznavanje izvanrazdiobnih primjera
- Zaključak

Izražavanje nesigurnosti predikcije

- Osnovne mjere za izražavanje nesigurnosti su vjerojatnost, entropija, diferencijalna entropija i varijanca.
- Neke mjere za izražavanje nesigurnosti predikcije kod klasifikacije su:
 - vjerojatnost klase s najvećom vjerojatnošću

$$\max_{k} P(y = k \mid \boldsymbol{x}, \boldsymbol{\theta}) \tag{1}$$

entropija

$$H(y \mid \boldsymbol{x}, \boldsymbol{\theta}) = - \underbrace{\mathbf{E}}_{y \mid \boldsymbol{x}, \boldsymbol{\theta}} \ln P(y \mid \boldsymbol{x}, \boldsymbol{\theta}). \tag{2}$$

 Ove mjere same po sebi ne razlikuju epistemičku i aleatornu nesigurnost.

Izražavanje nesigurnosti predikcije

• Rawat et al. [11], Smith i Gal [12] kao mjeru epistemičke nesigurnosti predikcije predlažu **međusobnu informaciju između izlazne** razdiobe i aposteriorne razdiobe parametara:

$$\underbrace{\mathbf{I}((y \mid \boldsymbol{x}, \mathcal{D}); (\boldsymbol{\theta} \mid \mathcal{D}))}_{U_{\mathsf{E}}} = \mathbf{H}(y \mid \boldsymbol{x}, \mathcal{D}) - \mathbf{H}((y \mid \boldsymbol{x}, \mathcal{D}) \mid (\boldsymbol{\theta} \mid \mathcal{D})) \quad (3)$$

$$= \underbrace{\mathbf{H}(y \mid \boldsymbol{x}, \mathcal{D})}_{U} - \underbrace{\mathbf{E}}_{\boldsymbol{\theta} \mid \mathcal{D}} \mathbf{H}(y \mid \boldsymbol{x}, \boldsymbol{\theta}). \quad (4)$$

- Zadnji izraz je razlika entropije predikcije i očekivanja entropije predikcije po aposteriornoj razdiobi parametara.
- To se može interpretirati kao očekivano znanje o parametrima koje se dobije ako se dobije oznaka za primjer x (to se može bolje vidjeti ako se međusobna informacija drugačije izrazi).

Aproksimacija bayesovske neuronske mreže pomoću dropouta

- Gal i Ghahramani [3] učenje s *dropoutom* interpretiraju kao varijacijsko zaključivanje.
- Ako pretpostavimo da dropout dolazi iza slojeva linearne transformacije, slučajne varijable koje odgovaraju varijacijskoj razdiobi matrica težina su

$$\boldsymbol{W}_l = \operatorname{diag}(\boldsymbol{z}_l) \boldsymbol{M}_l, \tag{5}$$

gdje je l indeks sloja, M_l matrica varijacijskih parametara, a z_l slučajni vektor čiji elementi su nezavisne slučajne varijable s Bernoullijevom razdiobom.

• Može se pokazati da minimizaciji $D_{KL}(q_{\phi} \parallel p(\theta \mid D))$, gdje je q_{ϕ} varijacijska razdioba, po varijacijskim parametrima ϕ , odgovara minimizacija uobičajene funkcije pogreške kod učenja s dropoutom.

Aproksimacija bayesovske neuronske mreže pomoću dropouta

 Obično se pri ispitivanju modela učenog s dropoutom ne koristi isključivanje jedinica, nego se parametri skaliraju vjerojatnošću neisključivanja, tj. procjenjuju se očekivanjem varijacijske razdiobe:

$$p(y \mid \boldsymbol{x}, \mathbb{D}) \approx p\left(y \mid \boldsymbol{x}, \boldsymbol{\theta} = \underset{\tilde{\boldsymbol{\theta}} \sim q_{\boldsymbol{\phi}}}{\mathbf{E}} \tilde{\boldsymbol{\theta}}\right).$$
 (6)

Ispravniji, ali manje efikasan način usrednjavanja je očekivanje izlaza
po varijacijskoj razdiobi parametara, što se može procijeniti sredinom
nekog broja uzoraka izlaza uz dropout [13, 2] – Monte Carlo dropout
(MC-dropout):

$$p(\boldsymbol{y} \mid \boldsymbol{x}, \mathbb{D}) \approx \underset{\tilde{\boldsymbol{\theta}} \sim q_{\boldsymbol{\phi}}}{\mathbf{E}} p(\boldsymbol{y} \mid \boldsymbol{x}, \tilde{\boldsymbol{\theta}}) \approx \frac{1}{M} \sum_{i=1}^{M} p(\boldsymbol{y} \mid \boldsymbol{x}, \boldsymbol{\theta} = \tilde{\boldsymbol{\theta}}_i),$$
 (7)

gdje su $\tilde{\theta}_i$ uzorci parametara iz varijacijske razdiobe q_{ϕ} .

- 1 Procjena nesigurnosti kod dubokih modela
- 2 Izražavanje nesigurnosti predikcije
- 3 Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita
- Eksperimenti: procjena nesigurnosti kod semantičke segmentacije pomoću dropouta
- **6** Eksperimenti: prepoznavanje izvanrazdiobnih primjera
- Zaključak

Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita

- Razdiobe koje duboki modeli daju kao izlaz softmaksa često pokazuju preveliku sigurnost.
- Hendrycks i Gimpel [6] pokazuju da se krivo klasificirani i izvanrazdiobni primjeri ipak mogu uspješno prepoznavati klasifikacijom maksimalne vjerojatnosti softmaksa.
- Guo et al. [5] pokazuju da se temperaturnim skaliranjem softmaksa, tj. dijeljenje logita skalarom T prije softmaksa, može značajno poboljšati kalibracija izlazne razdiobe već naučene mreže.

Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita

- Liang et al. [9] predlažu 2 poboljšanja klasifikacije maksimalne vrijednosti softmaksa za prepoznavanje izvanrazdiobnih primjera:
- Jedno poboljšanje je temperaturno skaliranje.
- Pokazuju da, što je temperatura veća, to se izvanrazdiobni primjeri mogu bolje odvojiti od unutarrazdiobnih primjera na temelju maksimalne vrijednosti softmaksa.
- Drugo poboljšanje je izmjena ulaza mreže tako da se FGSM-om pomakne u smjeru povećanja maksimalnog izlaza softmaksa:

$$\tilde{x} = x - \epsilon \operatorname{sgn} \nabla_x \left(-\ln \max_k p(y = k \mid x, \theta) \right).$$
 (8)

- Procjena nesigurnosti kod dubokih modela
- 2 Izražavanje nesigurnosti predikcije
- Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita
- **⚠** Eksperimenti: procjena nesigurnosti kod semantičke segmentacije pomoću dropouta
- **6** Eksperimenti: prepoznavanje izvanrazdiobnih primjera
- Zaključak

- Neka su $\{ ilde{ heta}_i\}_{i=1..M}$ uzorci iz varijacijske razdiobe *dropouta*.
- Monte Carlo aproksimacija hipoteze je $\overline{h}(m{x})\coloneqq \frac{1}{M}\sum_{i=1}^M h(m{x}; ilde{m{ heta}}_i).$
- Procjene ukupne, aleatorne i epistemičke nesigurnosti su:

$$U = H(y \mid \boldsymbol{x}, D) \approx -\overline{h}(\boldsymbol{x})^{\mathsf{T}} \ln(\overline{h}(\boldsymbol{x})),$$
 (9)

$$U_{\mathsf{A}} = \mathop{\mathbf{E}}_{\boldsymbol{\theta}\mid\mathbb{D}} \mathsf{H}(y\mid\boldsymbol{x},\boldsymbol{\theta}) \approx \frac{1}{M} \sum_{i=1}^{M} \mathsf{H}(y\mid\boldsymbol{x},\boldsymbol{\theta} = \tilde{\boldsymbol{\theta}}_i),$$
 (10)

$$U_{\mathsf{E}} = U - U_{\mathsf{A}},\tag{11}$$

gdje je $H(y \mid x, \theta = \tilde{\theta}_i) = -h(x; \tilde{\theta}_i)^T \ln(h(x; \tilde{\theta}_i))$ entropija razdiobe izlaza softmaksa *i*-tog uzorka.

- Korištena je vlastita implementacija mreže LadderDenseNet-121 za semantičku segmentaciju.
- Za dio mreže koji čini DenseNet-121 korištena je inicijalizacija parametrima mreže učene na ImageNet-u.
- Korišten je *dropout* s vjerojatnošću isključivanja 0.2.
- Za MC-dropout je kao kod Kendall i Gal [7] korišteno po M=50 uzoraka za procjenu izlazne razdiobe klasa i nesigurnosti za svaki primjer.

Model	mIoU/%	A/%
FC-DenseNet + dropout (Kendall i Gal [7])	67.1	-
+ aleatorna nesigurnost	67.2	-
+ MC-dropout	67.3	-
+ aleatorna nesigurnost i <i>MC-dropout</i>	67.4	-
LadderDenseNet-121-V	67.78(0.23)	91.65(0.07)
+ dropout	67.83(0.13)	91.29(0.18)
+ MC-dropout	67.98(0.18)	91.52(0.14)

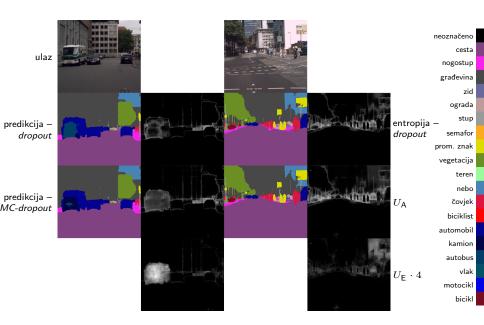
Tablica 1: Usporedba rezultata evaluacije na skupu CamVid. Vrijednosti za LadderDenseNet-121-V bez *dropouta* su prosjek 5 evaluacija.

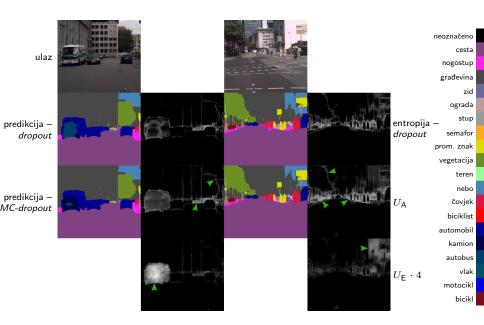
Model	mIoU/%	A/%
LadderDenseNet-121 [8]	72.82	95.06
LadderDenseNet-121-V + dropout	67.21(0.70) 62.82(0.75)	94.59(0.06) 93.44(0.06)
+ MC-dropout	64.16(0.45)	93.90(0.04)

Tablica 2: Usporedba rezultata evaluacije na validacijskom skupu Cityscapesa. Vrijednosti su prosjek 5 evaluacija. U zagradama su standardne devijacije.

Skup za učenje	Skup za testiranje	m Io U/%	U_{E}	U_{A}	$rac{U_{E}}{U_{A}}$
CamVid _{trainval} CamVid _{trainval,1/2} CamVid _{trainval,1/4} CamVid _{trainval,1/8}	$\begin{array}{c} CamVid_{test} \\ CamVid_{test} \\ CamVid_{test} \\ CamVid_{test} \end{array}$	66.3 61.5 54.6 46.0	0.025 0.026 0.029 0.034	0.207 0.272 0.391 0.538	0.121 0.097 0.073 0.063
CamVid _{trainval}	$CamVid_{val}$	82.7	0.011	0.118	0.093
CamVid _{trainval}	Cityscapes _{test} WildDash _{bench}	-	0.060 0.075	0.383 0.501	0.156 0.149
Cityscapes _{train} Cityscapes _{train} Cityscapes _{train}	Cityscapes _{val} Cityscapes _{test} WildDash _{bench}	64.4	0.024 0.020 0.153	0.187 0.162 0.600	0.126 0.122 0.254

Tablica 3: Srednje procjene epistemičke i aleatorne nesigurnosti za različite parove skupa za učenje i skupa za ispitivanje i njihovi omjeri.





- 1 Procjena nesigurnosti kod dubokih modela
- 2 Izražavanje nesigurnosti predikcije
- 9 Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita
- Eksperimenti: procjena nesigurnosti kod semantičke segmentacije pomoću dropouta
- **6** Eksperimenti: prepoznavanje izvanrazdiobnih primjera
- 6 Zaključak

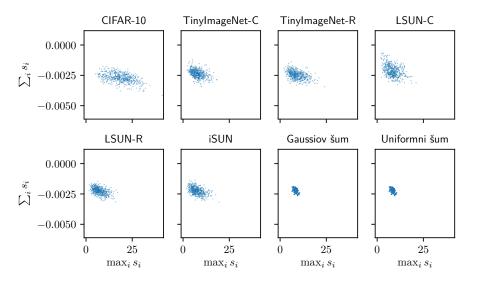
Eksperimenti: prepoznavanje izvanrazdiobnih primjera

- Liang et al. [9] pokazuju da su veće temperature bolje, pa se u eksperimentima s temperaturnim skaliranjem koristi T=1000.
- Kao pozitivna klasa se uzimaju unutarrazdiobni primjeri.
- Za svaki izvanrazdiobni skup se izdvaja 10% slika za odabir parametra pomaka ϵ minimizacijom FPR-a (učestalosti klasifikacije negativnih primjera kao pozitivnih) kad je odziv R=0.95.
- Ispitani su postupci klasifikacije:
 - $oldsymbol{0}$ po najvećoj vrijednosti softmaksa uz T=1 [6]
 - 2 po najvećoj vrijednosti softmaksa uz T=1000 [9]
 - 3 po najvećem logitu
 - 4 po najvećem normaliziranom logitu
 - 6 logističkom regresijom po zbroju i maksimalnoj vrijednosti logita
 - 6 logističkom regresijom po zbroju i maksimalnoj vrijednosti normaliziranih logita

uz i bez FGSM-a.

AUROC/%		WRN-28-10 $(A = 0.957)$
najveća vjerojatnost	92.4	90.5
najveća vjerojatnost, $T=1000$	95.7	93.1
najveća vjerojatnost, $T=1000$, FGSM	96.5	95.3
najveći logit	96.3	93.3
najveći logit, FGSM	96.5	95.3
najveći logit, FGSM	96.2	95.1
logistička regresija	96.4	95.5
logistička regresija, FGSM	97.0	95.5
najveći normalizirani logit	97.5	96.8
najveći normalizirani logit, FGSM	97.7	96.6
logistička regresija i normalizirani logiti	97.7	96.9
logistička regresija i normalizirani logiti, FGSM	97.8	96.9

Tablica 4: Prosječni AUROC na skupovima Tinylmagenet-C, Tinylmagenet-R, LSUN-C, LSUN-R, iSUN, *uniformni šum*, *gaussov šum*. Sufiks C znači da su nasumično izrezani dijelovi slika, a R da su slike smanjene na dimenzije 32×32 .



Slika 1: Odnos maksimalnog logita i zbroja logita za različite skupove kod mreže DenseNet-100-12.

- 1 Procjena nesigurnosti kod dubokih modela
- 2 Izražavanje nesigurnosti predikcije
- 9 Prepoznavanje izvanrazdiobnih i krivo klasificiranih primjera na temelju izlaza softmaksa ili logita
- Eksperimenti: procjena nesigurnosti kod semantičke segmentacije pomoću dropouta
- **6** Eksperimenti: prepoznavanje izvanrazdiobnih primjera
- 6 Zaključak

Zaključak

- Rezultati procjenjivanja epistemičke i aleatorne nesigurnosti uglavnom nisu u skladu s očekivanjem. Bilo bi dobro pokušati ih bolje razumjeti.
- Rezultati prepoznavanja izvanrazdiobnih primjera pokazuju da se performansa može poboljšati klasifikacijom na temelju većeg broja značajki izvedenih iz vektora logita.

Literatura

- [1] Armen Der Kiureghian i Ove Dalager Ditlevsen. Aleatoric or epistemic? Does it matter? Structural Safety, 31(2):105–112, 2009. ISSN 0167-4730. doi: 10.1016/j.strusafe.2008.06.020.
- [2] Yarin Gal i Zoubin Ghahramani. Dropout as a bayesian approximation: Representing model uncertainty in deep learning. svezak abs/1506.02142, 2015. URL http://arxiv.org/abs/1506.02142.
- [3] Yarin Gal i Zoubin Ghahramani. Bayesian convolutional neural networks with bernoulli approximate variational inference. svezak abs/1506.02158, 2015. URL http://arxiv.org/abs/1506.02158.
- [4] Ian J. Goodfellow, Jonathon Shlens, i Christian Szegedy. Explaining and harnessing adversarial examples. CoRR, abs/1412.6572, 2014. URL http://arxiv.org/abs/1412.6572.
- [5] Chuan Guo, Geoff Pleiss, Yu Sun, i Kilian Q. Weinberger. On calibration of modern neural networks. CoRR, abs/1706.04599, 2017. URL http://arxiv.org/abs/1706.04599.
- [6] Dan Hendrycks i Kevin Gimpel. A baseline for detecting misclassified and out-of-distribution examples in neural networks. *CoRR*, abs/1610.02136, 2016. URL http://arxiv.org/abs/1610.02136.
- [7] Alex Kendall i Yarin Gal. What uncertainties do we need in bayesian deep learning for computer vision? CoRR, abs/1703.04977, 2017. URL http://arxiv.org/abs/1703.04977.

Literatura

- [8] Ivan Krešo, Siniša Šegvic, i Josip Krapac. Ladder-style densenets for semantic segmentation of large natural images. U *The IEEE International Conference on Computer Vision (ICCV) Workshops*, Oct 2017.
- [9] Shiyu Liang, Yixuan Li, i R. Srikant. Principled detection of out-of-distribution examples in neural networks. CoRR, abs/1706.02690, 2017. URL http://arxiv.org/abs/1706.02690.
- [10] Anh Mai Nguyen, Jason Yosinski, i Jeff Clune. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. U CVPR, stranice 427–436. IEEE Computer Society, 2015. ISBN 978-1-4673-6964-0. URL http://dblp.uni-trier.de/db/conf/cvpr/cvpr2015.html#NguyenYC15.
- [11] Ambrish Rawat, Martin Wistuba, i Maria-Irina Nicolae. Adversarial phenomenon in the eyes of bayesian deep learning. arXiv preprint arXiv:1711.08244, 2017. URL https://arxiv.org/abs/1711.08244.
- [12] Lewis Smith i Yarin Gal. Understanding measures of uncertainty for adversarial example detection. CoRR, abs/1803.08533, 2018. URL http://arxiv.org/abs/1803.08533.
- [13] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, i Ruslan Salakhutdinov. Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15:1929–1958, 2014. URL http://jmlr.org/papers/v15/srivastava14a.html.
- [14] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian J. Goodfellow, i Rob Fergus. Intriguing properties of neural networks. *CoRR*, abs/1312.6199, 2013. URL http://arxiv.org/abs/1312.6199.

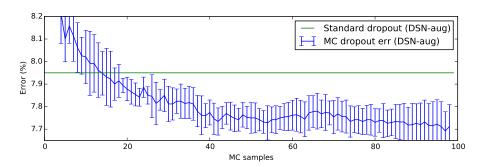
Međusobna informacija kao mjera epistemičke nesigurnosti

Tu međusobnu informaciju možemo i ovako izraziti:

$$I((y \mid \boldsymbol{x}, \mathbb{D}); (\boldsymbol{\theta} \mid \mathbb{D})) = H(\boldsymbol{\theta} \mid \mathbb{D}) - H((\boldsymbol{\theta} \mid \mathbb{D}) \mid (y \mid \boldsymbol{x}, \mathbb{D}))$$
(12)
$$= H(\boldsymbol{\theta} \mid \mathbb{D}) - H((\boldsymbol{\theta} \mid \boldsymbol{x}, \mathbb{D}) \mid (y \mid \boldsymbol{x}, \mathbb{D}))$$
(13)
$$= H(\boldsymbol{\theta} \mid \mathbb{D}) - \underset{v \mid \boldsymbol{x}, \mathbb{D}}{\mathbb{E}} H(\boldsymbol{\theta} \mid \boldsymbol{x}, y, \mathbb{D}).$$
(14)

- Zadnji izraz je razlika entropije aposteriorne razdiobe parametara i očekivanja entropije aposteriorne razdiobe parametara ako se u podatke uključi označeni primjer x.
- To možemo interpretirati kao očekivano znanje o parametrima koje dobijemo ako dobijemo oznaku za primjer x.

Aproksimacija bayesovske neuronske mreže pomoću dropouta



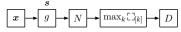
Slika 2: Ovisnost klasifikacijske pogreške (plavo) o broju uzoraka u *Monte Carlo* aproksimaciji izlaza na konvolucijskoj mreži koju su ispitivali autori [3] na skupu CIFAR-10. Svaka točka je prosjek 5 mjerenja i prikazane su standardne devijacije. Zeleni pravac označava klasifikacijsku pogrešku kod uobičajenog usrednjavanja skaliranjem težina. Slika je preuzeta iz Gal i Ghahramani [3].



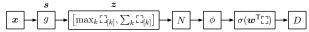
(a) Klasifikacija po maksimalnoj vrijednosti softmaksa.

$$x \longrightarrow g \longrightarrow \max_{k} \square_{[k]} \longrightarrow D$$

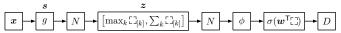
(b) Klasifikacija po maksimalnom logitu.



(c) Klasifikacija po maksimalnom normaliziranom logitu.



(d) Klasifikacija para koji čine maksimalni logit i zbroj logita logističkom regresijom s normalizacijom i polinomijalnim baznim funkcijama stupnjeva od 0 do 2.



(e) Klasifikacija para koji čine maksimalni normalizirani logit i zbroj normaliziranih logita logističkom regresijom s normalizacijom i polinomijalnim baznim funkcijama sa stupnjevima od 0 do 2.

Slika 3: Grafički prikaz postupaka za klasifikaciju na temelju logita ili softmaksa. $g: x \mapsto s$ je funkcija koja ulaz preslikava u vektor logita. N je funkcija koja normalizira vektor po svakoj komponenti posebno oduzimanjem sredine i dijeljenjem sa standardnom devijacijom prema izdvojenim skupovima. $\phi: [a,b] \mapsto [1,a,b,a^2,b^2,ab]$ je funkcija polinomijalnih značajki sa stupnjevima od 0 do 2. D je funkcija koja određuje pripada li primjer razdiobi skupa za učenie usporedbom ulaza s pragom.