**ŽILINSKÁ UNIVERZITA V ŽILINE**

# AUTOREFERÁT
DIZERTAČNEJ PRÁCE

**Žilina, máj 2023**

Ing. René Fabricius

**Žilinská univerzita v Žiline**
**Fakulta riadenia a informatiky**

**Ing. René Fabricius**

Autoreferát dizertačnej práce
# Teória a aplikácie párových ansámblových modelov

na získanie akademického titulu "**philosophiae doctor**" (**PhD.**)
v študijnom programe doktorandského štúdia
**aplikovaná informatika**

v študijnom odbore
**informatika**

Žilina, máj 2023

**Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia na Katedre matematických metód a operačnej analýzy, Fakulte riadenia a informatiky Žilinskej univerzity v Žiline**


**Predkladateľ:** *Ing.* ***René Fabricius***
Katedra matematických metód a operačnej analýzy
Fakulta riadenia a informatiky
Žilinská univerzita v Žiline

**Školiteľ:** *doc. Mgr.* ***Ondrej Šuch****, PhD.*
Matematický ústav Slovenskej akadémie vied
Banská Bystrica

**Školiteľ špecialista:** *Ing.* ***Peter Tarábek****, PhD.*
Katedra matematických metód a operačnej analýzy
Fakulta riadenia a informatiky
Žilinská univerzita v Žiline

**Oponenti:** *prof. Ing.* ***Igor Farkaš****, Dr.*
Fakulta matematiky, fyziky a informatiky
Univerzita Komenského v Bratislave

*doc. Ing.* ***Tomáš Kliegr****, PhD.*
Fakulta informatiky a statistiky
Vysoká škola ekonomická v Praze



**Autoreferát bol rozoslaný dňa: 4. 7. 2023**


Obhajoba dizertačnej práce sa koná dňa **23.8.2023** o **11.00** hod. pred komisiou pre obhajobu dizertačnej práce schválenou pracovnou skupinou odborovej komisie v študijnom odbore **informatika**, v študijnom programe **aplikovaná informatika**, vymenovanou dekanom Fakulty riadenia a informatiky Žilinskej univerzity v Žiline dňa **3. 7. 2023**.

*prof. Ing.* ***Karol Matiaško****, PhD.*
predseda pracovnej skupiny odborovej komisie
v študijnom odbore **informatika**
v študijnom programe **aplikovaná informatika**


Fakulta riadenia a informatiky
Žilinská univerzita
Univerzitná 8215/1
010 26 Žilina

# Anotácia

Klasifikačné ansámblové modely produkujú klasifikačné predikcie pomocou kombinácie viacerých klasifikačných algoritmov. Ansámblové modely sú z dôvodu svojej robustnosti a presnosti súčasťou oblasti strojového učenia už od jej počiatkov. Ich hlavnou výhodou je schopnosť kombinovať rôznorodé predikcie svojich členov a získať tak predikciu často lepšiu, ako by vyprodukoval ktorýkoľvek člen samostatne. V úvode práce poskytujeme prehľad existujúcich ansámblových metód, ich vlastností a stavebných blokov, špeciálnu pozornosť venujeme párovým ansámblovým modelom. Jadrom práce je tvorba novej parametrickej ansámblovej metódy využívajúcej binarizáciu. Metóda priraďuje váhy jednotlivým dvojiciam tried každého kombinovaného klasifikátora. Navrhovanú metódu nazývame Vážený lineárny ansámbel (WLE). Práca zahŕňa návrh metódy, tvorbu metodológie jej trénovania a použitia, ladenie hyperparametrov metódy a otestovanie metódy na niekoľkých datasetoch. Na datasetoch CIFAR-100 a ImageNet porovnávame navrhovanú metódu s populárnym priemerovacím ansámblom. Výsledky týchto experimentov ukazujú, že navrhovaná metóda vo väčšine prípadov produkuje kvalitnejšie predikcie. V práci skúmame tiež možnosť využitia WLE metódy na detekciu neznámych vzoriek a porovnávame ju so zaužívanými prístupmi na riešenie tejto úlohy. Experimenty na úlohe rozlišovania medzi datasetmi CIFAR-10 a CIFAR-100 ukazujú, že aplikácia metódy maximálnej predikovanej pravdepodobnosti na výstupy WLE poskytuje lepšiu detekciu neznámych vzoriek, ako aplikácie tej istej metódy na výstupy priemerovacieho ansámblu.

**Kľúčové slová**: klasifikačná úloha, lineárne klasifikačné metódy, neurónové siete, ansámblové modely

| | | | |
|---|---|---|---|
| *Počet strán:* | *166* | *Počet použitej literatúry:* | *99* |
| *Počet obrázkov:* | *55* | *Počet tabuliek:* | *13* |

# 1 Úvod

Keď stojíme pred komplexnou a náročnou úlohou je bežnou praxou obrátiť sa na tím expertov s rozličnými relevantnými oblasťami expertízy. V súlade s porekadlom: "Viac hláv, viac rozumu", má takýto tím pri vhodnom spôsobe spolupráce väčšiu šancu dospieť k dobrému riešeniu, ako jednotliví jeho členovia samostatne.

Na základe podobnej filozofie sa v oblasti strojového učenia vytvárajú "tímy" predikčných modelov spolupracujúcich na riešení zadaného problému. Takéto "tímy" sa označujú pojmom ansámblové modely. Použitie ansámblového prístupu je umožnené existenciou veľkého množstva rôznorodých predikčných modelov, ktoré majú rozličné silné a slabé stránky.

V poslednom čase vo viacerých oblastiach strojového učenia prevláda použitie hlbokých umelých neurónových sietí (DNN). Rýchly vývoj v oblasti DNN má za následok dostupnosť veľkého množstva rozličných architektúr sietí s rôznymi vlastnosťami. Trénovanie takýchto sietí je stochastický proces, ktorý je možné do veľkej miery modifikovať a prispôsobiť nastavením rozličných parametrov, čo má za následok rozličné výsledné modely aj pri použití jednej architektúry. Tieto skutočnosti robia z DNN vhodných kandidátov na vytváranie ansámblových modelov.

Pre získanie výsledného rozhodnutia ansámblového modelu je potrebné skombinovať rozhodnutia jednotlivých jeho členov. Existuje veľké množstvo kombinačných metód, ktoré to umožňujú. Niektoré kombinačné metódy sú jednoduché algebraické pravidlá, iné zahŕňajú komplexné algoritmy, ktoré vyžadujú vlastné trénovanie. Výber vhodnej kombinačnej metódy záleží, ako od druhu riešenej úlohy, tak aj od typu kombinovaných modelov.

V úvode práce poskytujeme prehľad existujúcich ansámblových modelov, ich možné využitie a základné stavebné bloky. Zameriavame sa na klasifikačné úlohy. Naša pozornosť sa sústredí na druh ansámblov využívajúci binarizáciu, nazývaný tiež párové ansámble. Párové ansámble majú svoj pôvod pri kombinovaní inherentne dvojtriednych klasifikátorov za účelom viactriednej klasifikácie.

Jadrom práce je návrh novej párovej ansámblovej metódy. Na rozdiel od prvotných párových ansámblových metód, naša metóda kombinuje viactriedne klasifikátory a jej výstupom je tiež viactriedna klasifikácia. Súčasťou metódy je rozloženie vstupných klasifikátorov na dvojtriedne klasifikátory a ich následné kombinovanie. Navrhnutá metóda je rozšírená o funkcionalitu detekcie neznámych vzoriek.

Práca popisuje experimenty a ich výsledky, ktoré vedú k vybudovaniu metodiky použitia navrhnutej ansámblovej metódy a odladeniu jej hyperparametrov. Odladenú metódu porovnávame s existujúcou populárnou ansámblovou metódou. Venujeme sa tiež otestovaniu funkcionality detekcie neznámych vzoriek.

V závere práce sú zhrnuté dosiahnuté výsledky a je načrtnuté ďalšie možné smerovanie výskumu.

# 2 Teoretické východiská a súčasný stav

Ansámblové metódy je možné využiť na riešenie ako regresných, tak aj klasifikačných úloh. Pri aplikácii ansámblovej klasifikačnej metódy sa kombinuje niekoľko individuálnych klasifikátorov. Tieto klasifikátory môžu patriť do rovnakého druhu, vtedy hovoríme o homogénnych ansámbloch, alebo do rozličných druhov, vtedy ide o heterogénne ansámble.

Ansámblové modely rôznych druhov našli uplatnenie vo viacerých praktických aplikáciách. Niekoľko príkladov je: vyhodnocovanie kvality senzorických dát [1], rozpoznávanie osôb v interiéri áut [2] a rozličné medicínske aplikácie ako predikcia biologickej aktivity farmaceutických molekúl [3], určovanie regiónov dôležitých pre klasifikáciu v spektre magnetickej rezonancie [4] alebo diagnóza rakoviny prsníka [5].

Aby mohla ansámblová metóda vyprodukovať klasifikátor poskytujúci lepšiu predikciu ako individuálne klasifikátory, musia byť chyby, ktoré tieto klasifikátory robia, rozličné [6]. Bolo vyvinutých veľa rôznych metód, ktoré sa usilujú zabezpečiť diverzitu trénovaných klasifikátorov. Štandardne tieto metódy modifikujú trénovací proces členov ansámblu. Autori v [7] interpretujú trénovací proces ako prehľadávanie množiny hypotéz, ktoré môže model reprezentovať. Metódy na zabezpečenie diverzity rozdelili do troch hlavných kategórií podľa toho, akým spôsobom pracujú:

- modifikácia štartovacieho bodu prehľadávania v priestore hypotéz,
- modifikácia množiny dostupných hypotéz,
- modifikácia spôsobu prehľadávania množiny hypotéz.

Ansámblové modely sú často schopné dosahovať presnejšie a robustnejšie predikcie ako individuálne klasifikátory. Tu uvádzame niekoľko teoretických príčin sformulovaných v [8], ktoré zdôvodňujú prečo tomu tak je.

**Reprezentačná výhoda** je spôsobená obmedzenými reprezentačnými schopnosťami jednotlivých modelov v dôsledku ich architektúry, alebo obmedzeného množstva trénovacích dát.

**Štatistická výhoda** je spôsobená obmedzeným množstvom dát na testovanie jednotlivých modelov a výber najlepšieho z nich.

**Výpočtová výhoda** sa prejavuje v dôsledku stochastickej a heuristickej povahy trénovacieho procesu jednotlivých modelov.

## 2.1 Metódy kombinovania klasifikátorov

Metódy kombinovania klasifikátorov kombinujú výstupy natrénovaných členov ansámblu a produkujú tak finálnu predikciu ansámblového modelu. Metódy kombinovania klasifikátorov môžeme rozdeliť do dvoch skupín na:

- metódy bez trénovania,
- metódy s trénovaním.

Metódy bez trénovania sú jednoduchšie, neumožňujú ale zohľadniť vlastnosti jednotlivých členov ansámblu. Metódy s trénovaním sú zvyčajne úspešnejšie keď majú jednotlivé členy ansámblu rozdielnu presnosť, alebo keď spracúvajú rozličné množiny príznakov [9].

### 2.1.1 Metódy bez trénovania

**Metódy bez trénovania** sú napriek svojej jednoduchosti často využívané a môžu byť tiež použité ako referencia pri testovaní zložitejších metód. V nasledujúcom texte je uvedených niekoľko takýchto metód.

Pri použití metódy **väčšinové hlasovanie** priradí ansámbel pozorovanie do tej triedy, pre ktorú hlasuje väčšina členov ansámblu. Matematické vyjadrenie klasifikácie pozorovania $\boldsymbol{x}$ pri väčšinovom hlasovaní je

$$Class(\boldsymbol{x}) = \arg\max_{k \in K} \sum_{c \in C} d_k^c(\boldsymbol{x}), \tag{1}$$

kde $K$ je množina klasifikovaných tried, $C$ je množina členov ansámblu a $d_k^c(\boldsymbol{x})$ je rozhodnutie klasifikátora $c$ o triede $k$. $d_k^c(\boldsymbol{x})$ nadobúda hodnotu 1, ak klasifikátor $c$ zaradil pozorovanie $\boldsymbol{x}$ do triedy $k$, inak nadobúda hodnotu 0.

**Súčet rozdelení pravdepodobnosti** je možné použiť v prípade, že členy ansámblu produkujú ako svoj výstup rozdelenia pravdepodobnosti [9]. Pokiaľ pri neurónovej sieti $c$ použijeme ako výstupnú aktivačnú funkciu softmax, môžeme jej výstupy interpretovať ako pravdepodobnosti príslušnosti do jednotlivých tried: $f_k^c(\boldsymbol{x}) = \hat{P}_c(Y = k|\boldsymbol{x})$. Potom výslednú klasifikáciu určíme ako

$$Class(\boldsymbol{x}) = \arg\max_{k \in K} \sum_{c \in C} f_k^c(\boldsymbol{x}). \tag{2}$$

Pri výstupoch členov ansámblu vo forme rozdelení pravdepodobnosti môžeme použiť tiež rôzne algebraické kombinačné metódy uvedené v [10].

### 2.1.2 Metódy s trénovaním

Metódy s trénovaním sú zväčša komplikovanejšie ako metódy bez trénovania, poskytujú ale lepšie možnosti prispôsobenia sa vlastnostiam kombinovaných klasifikátorov. Tieto metódy často zahŕňajú použitie viacerých úrovní modelov štatistického učenia. Základnými príkladmi takýchto metód sú:

- **Stohovanie** (ang. stacking) používa dvojúrovňovú klasifikáciu. Prvá úroveň pozostáva z klasických členov ansámblu a druhá úroveň je meta-klasifikátor. Výstup meta-klasifikátora je finálnym výstupom ansámblu [9].

- **Triedenie** (ang. grading) je ďalšia metóda, ktorá sa dá chápať ako dvojúrovňová. V prípade triedenia je ku každému klasifikátoru priradený osobitný meta-klasifikátor. Meta-klasifikátory pre každé pozorovanie predikujú, či im priradený klasifikátor správne určí triedu daného pozorovania [11].

- **Bránovanie** (ang. gating) je podobná metóda ako triedenie s tým rozdielom, že využíva len jeden meta-klasifikátor, nazývaný bránovací (ang. gating) klasifikátor. Výstupom bránovacieho klasifikátora sú pravdepodobnosti toho, že jednotlivé členy ansámblu vyprodukujú pre dané vstupy správnu predikciu[12].

Existuje niekoľko zaužívaných ansámblových klasifikačných metód, ktoré špecifikujú typ použitých klasifikátorov, spôsob ich trénovania, metódu zabezpečenia diverzity a tiež metódu kombinovania klasifikátorov. Rôzne metódy umožňujú vykonávať rôznu mieru zmien v týchto základných stavebných blokoch. Tieto metódy môžeme rozdeliť do dvoch kategórií: závislé a nezávislé.

Závislé metódy využívajú pri trénovaní členov ansámblu informácie, ktoré im poskytujú výstupy už natrénovaných členov. Do tejto kategórie patria metódy založené na princípe **Boosting** [13].

Nezávislé metódy trénujú všetky členy nezávisle, príkladom takejto metódy je **Bagging** [14].

## 2.2 Párové ansámblové modely

Párové ansámblové modely sú viactriedne klasifikačné modely, ktoré sú zostavené z pravdepodobnostných dvojtriednych klasifikátorov. Každý dvojtriedny klasifikátor rozlišuje medzi dvojicou tried viactriednej úlohy a ich výstupy sú kombinované pomocou špeciálnych párových zväzovacích metód [15, 16, 17].

### 2.2.1 Párové zväzovacie metódy

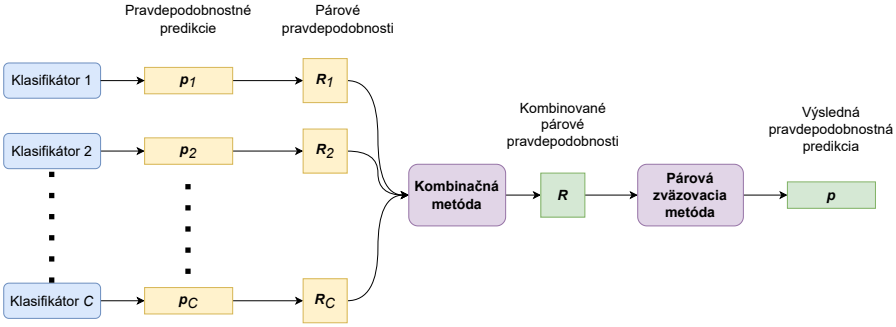
Párové zväzovacie (ang. pairwise coupling) metódy sú špeciálnym prípadom metód kombinovania klasifikátorov bez trénovania. V práci využívame dve metódy navrhnuté autormi Wu, Lin a Weng v článku [15], ktoré označujeme ako **m1** a **m2**, Bayesovsky kovariantnú metódu [17], ktorú označujeme ako **bc** a metódu od autorov Šuch, Benuš a Tinajová [16], ktorú označujeme ako **sbt**.

Tieto metódy predpokladajú, že pre každé pozorovanie $\boldsymbol{x}$ a označenie triedy $y$ máme k dispozícii výstupy dvojtriednych klasifikátorov $r_{ij}$, ktoré aproximujú pravdepodobnosti $\mu_{ij} = P(Y = i \mid Y = j \text{ alebo } Y = i, \boldsymbol{x})$. Cieľom párových kombinačných

metód je s pomocou všetkých $r_{ij}$ odhadnúť $\boldsymbol{p} = (p_1, p_2, \ldots, p_K)^T$ kde $p_i = P(Y = i \mid \boldsymbol{x})$.

# 3 Vážený lineárny ansámbel

V tejto sekcii sa venujeme návrhu novej ansámblovej metódy pomenovanej Vážený lineárny ansámbel (WLE). WLE metóda rieši úlohu viactriednej klasifikácie kombinovaním niekoľkých viactriednych klasifikátorov. Diagram činnosti metódy je zobrazený na obrázku 1. Metóda využíva postup **binarizácie**, pri ktorom rozdelí riešený problém na niekoľko dvojtriednych podproblémov. V kontexte týchto dvojtriednych podproblémov skombinuje predikcie členov ansámblu pomocou **kombinačnej metódy**. Získané dvojtriedne predikcie metóda skombinuje použitím **párovej zväzovacej metódy** a získa tak výslednú viactriednu pravdepodobnostnú klasifikáciu.



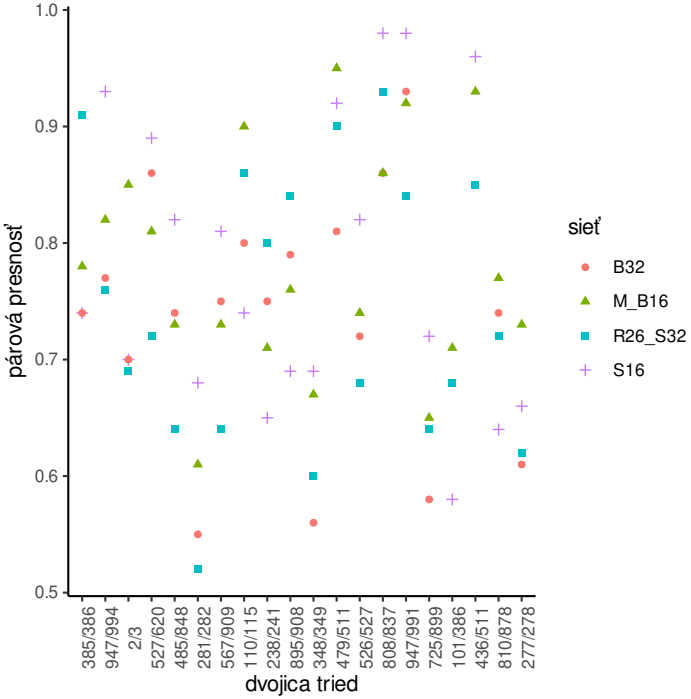

**Obr. 1:** Diagram činnosti WLE metódy.

Postup získania dvojtriednych predikcií zo vstupných viactriednych predikcií je založený na predpoklade platnosti axiómu irelevantných alternatív. Ak vektor $\boldsymbol{p} = (p_1, p_2, \ldots, p_K)$ je výstup viactriedneho pravdepodobnostného klasifikátora a $p_i$ predstavuje pravdepodobnosť príslušnosti klasifikovaného objektu do triedy $i$, potom výstup dvojtriedneho klasifikátora rozlišujúceho medzi triedami $i$ a $j$ môžeme vyjadriť ako

$$\left( \frac{p_i}{p_i + p_j}, \frac{p_j}{p_i + p_j} \right). \tag{3}$$

Motivácia pre kombinovanie viactriednych klasifikátorov s využitím transformácie na dvojtriedne klasifikátory spočíva v tom, že rôzne klasifikátory môžu mať rozličné schopnosti rozlišovať medzi jednotlivými dvojicami tried. Takúto situáciu

vidíme na obrázku 2. Na obrázku môžeme vidieť veľké rozdiely medzi párovými presnosťami jednotlivých sietí. Tiež môžeme pozorovať, že poradie sietí podľa párových presností sa pre rôzne dvojice tried líši.




**Obr. 2:** Párové presnosti štyroch neurónových sietí na datasete ImageNet1k. Presnosti sú zobrazené pre 20 párov tried s najvyššími rozptylmi v párových presnostiach skúmaných sietí. Označenia tried reprezentujú poradie (indexované od nuly) zodpovedajúceho priečinku medzi abecedne zoradenými priečinkami tried Imagenet1k datasetu.

Párové predikcie, ktoré získame pomocou binarizácie je potrebné zlúčiť do jednej matice párových predikcií, ktorá slúži ako vstup do párových zväzovacích metód. Za týmto účelom sme navrhli niekoľko kombinačných metód, ktoré predstavíme v nasledujúcej podsekcii.

## 3.1 Kombinačné metódy

Ako vstup do kombinačných metód používame výstupy poslednej vrstvy neurónových sietí pred aplikovaním funkcie softmax, nazývané logity. Pri klasifikácii má po-

sledná vrstva štandardne rovnaký počet výstupov, ako je počet tried. Logity kombinovaných klasifikátorov $1,2,\ldots,C$ označujeme ako $\boldsymbol{l}^1,\boldsymbol{l}^2,\ldots,\boldsymbol{l}^C$, kde $\boldsymbol{l}^c=(l_1^c,l_2^c,\ldots,l_K^c)$ pre jednotlivé triedy $1,2,\ldots,K$. V technickom prevedení kombinujeme rozdiely logitov, čo je ekvivalentný prístup k použitiu párových pravdepodobností z rovnice (3).

Výstupom kombinačných metód je matica párových pravdepodobností $\boldsymbol{R}$, ktorá je vstupom pre párové zväzovacie metódy. Istým spôsobom sa tento krok nášho ansámblového modelu dá považovať za **stohovací** ansámbel a kombinačné metódy za metaklasifikátor.

Kombinačné metódy, ktoré sme navrhli možno rozdeliť do dvoch hlavných kategórií:

- bezparametrické,
- parametrické.

Bezparametrické metódy nevyžadujú trénovanie a teda ani žiadne dáta navyše. Parametrické metódy používajú na kombinovanie klasifikátorov parametre, pre ktoré je potrebné nájsť vhodné hodnoty trénovaním. V nasledujúcom texte opíšeme niektoré z metód, ktoré sme implementovali a testovali.

**Bezparametrické metódy**, ktoré sme implementovali sú založené na priemerovaní. Tieto metódy dosahovali horšie výsledky ako parametrické metódy, ich bližší opis tu preto neposkytujeme.

**Parametrické metódy** využívajú pri kombinovaní klasifikátorov trénovateľné parametre. Kombinácia je lineárna vzhľadom na parameter funkcie expit. Matematicky môžeme výpočet vyjadriť ako

$$r_{ij}=\operatorname{expit}\Big(\sum_{c=1}^{C} w_{ij}^c(l_i^c-l_j^c)+b_{ij}\Big) \tag{4}$$

kde $r_{ij}$ je prvok výstupnej matice $\boldsymbol{R}$, $w_{ij}^c$ je koeficient prislúchajúci k dvojici tried $i,j$ a klasifikátoru $c$ a $b_{ij}$ je bias prislúchajúci k dvojici tried $i,j$. Jednotlivé kombinačné metódy sa líšia v tom, akým spôsobom nastavujú hodnoty kombinačných koeficientov.

### 3.1.1 Logistická regresia

Kombinačná metóda **logreg** využíva na určenie hodnôt koeficientov klasifikačný algoritmus **logistická regresia**. Logistická regresia rieši pre každú dvojicu tried $\{i,j\}$ dvojtriednu klasifikačnú úlohu. Prediktory v tejto úlohe sú rozdiely logitov pre jednotlivé kombinované klasifikátory $l_i^c-l_j^c$ pre $c=1,2,\ldots,C$. Výsledné parametre sú určené parametrami natrénovaného modelu.

Základná kombinačná metóda **logreg** trénuje aj bias a používa $l_2$ regularizáciu. Variant **logreg_no_interc** trénuje model bez biasu, koeficienty $b_{ij}$ teda ostávajú nulové, a taktiež používa $l_2$ regularizáciu.

### 3.1.2 Gradientové metódy

Ďalšia skupina kombinačných metód využíva takzvané end-to-end trénovanie. Hodnoty kombinačných koeficientov sú v tomto prípade určované na základe výslednej pravdepodobnostnej klasifikácie vystupujúcej z párovej zväzovacej metódy. Trénovanie je realizované pomocou metódy stochastického gradientového zostupu (ang. stochastic gradient descent) (SGD) a s použitím stratovej funkcie metódy maximálnej vierohodnosti (ang. negative log likelihood) (NLL). Tieto kombinačné metódy sú označované ako **grad_m1**, **grad_m2**, **grad_bc** a **grad_sbt**, kde časť názvu za podčiarkovníkom zodpovedá označeniu párovej zväzovacej metódy použitej pri trénovaní. Pri predikcii môžu byť koeficienty získané pomocou týchto metód použité aj s inou párovou zväzovacou metódou ako bola použitá pri trénovaní, rovnako ako pri ostatných kombinačných metódach.

## 3.2 Detekcia neznámych vzoriek

Kľúčovým problémom väčšiny moderných klasifikátorov je, že sú natrénované na obmedzenú množinu tried a pri klasifikovaní vzorky, ktorá nespadá do tejto množiny je ich výstup nevyhnutne nesprávny. Tento problém sa snaží riešiť funkcionalita detekcie neznámych vzoriek (ang. out of distribution (OOD) detection), ktorá umožňuje klasifikátoru vyhodnotiť vzorku ako neznámu a nezaradiť ju do žiadnej z tried na ktoré bol natrénovaný.

OOD detekciu je možné realizovať ak klasifiátor dokáže kvantifikovať istotu, prípadne neistotu, s vykonanou predikciou. Na základe výstupov na vhodnej validačnej množine a so zohľadnením požiadaviek riešeného problému je potom možné zvoliť hraničnú hodnotu istoty (resp. neistoty). Predikcie s istotou (resp. neistotou) na jednej strane tejto hraničnej hodnoty sú považované za platné a predikcie na druhej strane sú považované za detekovanú neznámu vzorku.

Jeden zo základných prístupov, ktorý vykazuje dobrú úspešnosť v rozličných aplikáciách [18], modeluje istotu (ang. confidence) modelu pomocou maximálnej hodnoty spomedzi pravdepodobností na jeho výstupe. V našich experimentoch tento prístup označujeme ako MSP (ang. maximum softmax probability).

Použitie párových zväzovacích metód otvára možnosti využitiu nových prístupov ku kvantifikovaniu istoty resp. neistoty klasifikátora s vykonanou predikciou. Párové zväzovacie metódy kombinujú párové predikcie poskytujúce redundantné informácie. Tieto informácie sú vo väčšine prípadov nekonzistentné. Pri párových zvä-

zovacích metódach **m1**, **m2** a **bc** je možné túto nekonzistenciu kvantifikovať. Mieru nekonzistencie využívame ako neistotu s vykonanou predikciou.

### 3.3 Predikcia pri úlohách s veľkým počtom tried

Výpočtová a pamäťová náročnosť kombinačných metód ako aj párových zväzovacích metód, z ktorých sa WLE skladá rastie priamo úmerne s druhou mocninou počtu tried riešeného problému. Pri trénovaní kombinačných metód, ktoré pre každú dvojicu tried hľadajú hodnoty kombinačných parametrov sa nedokážeme vyhnúť spracovaniu všetkých dvojíc tried. Pri predikcii ale môžeme výpočtovú aj pamäťovú náročnosť ansámblovej predikcie znížiť s využitím výstupov kombinovaných klasifikátorov predtým ako ich poskytneme ansámblovému modelu.

Navrhli sme preto úpravu založenú na úvahe, že je nepravdepodobné, aby sa trieda, ktorá má u všetkých kombinovaných klasifikátorov nízku podporu dostala v ansámblovej predikcii medzi triedy s vysokou podporou. Úprava teda funguje tak, že vezme z každého z kombinovaných klasifikátorov stanovený počet tried s najvyššou podporou, vytvorí zjednotenie týchto tried a ansámblový model skombinuje predikcie len pre triedy v zjednotení. Zvyšné triedy majú vo výstupe ansámblového modelu nulovú pravdepodobnosť. Počet tried, ktoré sú vybrané pre každý z kombinovaných klasifikátorov je riadený hyperparametrom *topl*.

## 4 Popis experimentov a výsledkov

Lineárny vážený ansámbel (WLE), ktorý testujeme je tvorený kombináciou kombinačnej metódy a párovej zväzovacej metódy. Pre lepšiu prehľadnosť a stručnosť v nasledujúcich sekciách označujeme WLE ako konfigurácia kombinačná metóda + párová zväzovacia metóda. Teda napríklad ansámbel zložený z kombinačnej metódy **logreg** a párovej zväzovacej metódy **sbt** označíme ako konfigurácia **logreg + sbt**.

S metódou WLE sme vykonali viacero experimentov. Prvé experimenty boli zamerané na určenie vhodnej trénovacej metodológie parametrických kombinačných metód. Tieto experimenty sme vykonali na datasetoch CIFAR-10 a CIFAR-100. V experimentoch sme určili vhodnú veľkosť trénovacej množiny kombinačných metód ako 50 vzoriek na triedu riešeného problému. Zistili sme tiež lepšie výsledky pri trénovaní kombinačných metód na oddelenej validačnej množine oproti trénovaniu na trénovacej množine členov ansámblu.

V ďalších experimentoch sme porovnali veľké množstvo navrhnutých konfigurácií WLE a vybrali sme z nich niekoľko vhodných na ďalšie testovanie.

Následne sme odladili hyperparameter miery regularizácie v gradientových kombinačných metódach a v kombinačných metódach založených na logistickej regresii.

Odladené vybrané konfigurácie WLE sme porovnali s baseline ansámblom na datasete CIFAR-100. Popis tohto vyhodnotenia je v podsekcii 4.3.

Ďalšie experimenty sme vykonávali na datasete ImageNet. Pre jednotlivé konfigurácie WLE sme určili vhodné hodnoty hyperparametra riadiaceho zjednodušenú predikciu popísanú v podsekcii 3.3. Následne sme vybrané WLE konfigurácie porovnali s baseline ansámblom aj na datasete ImageNet. Tento experiment je popísaný v podsekcii 4.4.

Na záver popisujeme experimenty s funkcionalitou OOD detekcie. Popis týchto experimentov je v podsekcii 4.5.

Ako baseline ansámbel s ktorým porovnávame klasifikačné výsledky sme si zvolili priemer kalibrovaných predikcií členov ansámblu. Ide o jednoduchú a populárnu ansámblovú metódu.

## 4.1 Metriky na vyhodnocovanie kvality výsledkov

Pri vyhodnocovaní experimentov používame niekoľko metrík kvality. Klasická metrika pri klasifikácii je presnosť klasifikácie (ang. accuracy). Pri pravdepodobnostných klasifikátoroch existuje aj zovšeobecnenie presnosti na viac ako jednu najpravdepodobnejšiu triedu. Toto zovšeobecnenie sa nazýva *top-k* presnosť a vyjadruje u akej časti klasifikovaných vzoriek sa správna trieda nachádza medzi $k$ triedami s najvyššou predikovanou pravdepodobnosťou. Pri datasete ImageNet sa štandardne využívajú dve presnosti, *top-1* a *top-5*.

Ďalšia metrika, ktorá sa tiež často používa pri trénovaní neurónových sietí, je pokutová funkcia metódy maximálnej vierohodnosti (ang. negative log likelihood) (NLL).

Pre praktické použitie klasifikátora je potrebné aby bol dobre kalibrovaný. Mieru kalibračnej chyby meria metrika odhad kalibračnej chyby (ang. estimated calibration error) (ECE). Túto metriku počítame pomocou postupu popísaného v [19], konkrétne postupom s rovnakou početnosťou vzoriek v jednotlivých intervaloch.

V experimentoch sa venujeme tiež detekcii neznámych vzoriek (ang. out-of-distribution detection). Takúto úlohu je možné interpretovať ako dvojtriednu klasifikačnú úlohu.

Algoritmy, ktoré na OOD detekciu využívame poskytujú ako svoj výstup mieru príslušnosti do jednej z dvoch tried. Kvalitu výstupov takýchto klasifikátorov je možné charakterizovať pomocou krivky, ktorá sa nazýva operačná charakteristika prijímača (ROC z ang. Receiver Operating Characteristic). Ďalšia často využívaná krivka, nazývaná PR krivka, môže poskytnúť cenné informácie najmä v prípade nerovnomerného zastúpenia jednotlivých tried v datasete [20].

Porovnávanie viacerých klasifikátorov na základe týchto kriviek je obtiažne. Využívajú sa preto číselné metriky, ktoré merajú plochy pod spomínanými krivkami.

Pre krivku ROC sa táto metrika označuje ako AUROC a pre krivku PR ako AUPRC.

## 4.2 Kombinované klasifikátory

V experimentoch sme využívali neurónové siete s rozličnými architektúrami, aby sme zabezpečili dostatočnú diverzitu kombinovaných predikcií. Pri vyhodnocovaní na datasete CIFAR-100 sme použili neurónové siete: resnet34 [21], densenet121 [22] a xception [23]. Tieto siete sa trénujú klasickým spôsobom na trénovacej množine datasetu, pre ktorý sú použité. Okrem týchto sietí sme použili tiež predtrénovaný extraktor príznakov clip [24], konkrétne s architektúrou siete ViT-B-32. Na výstupe tohto extraktora príznakov sme na príslušnej trénovacej množine natrénovali multinomiálnu regresiu.

V sekcii venujúcej sa detekcii neznámych vzoriek využívame klasifikátory predtrénované na kompletnom datasete ImageNet21k [25] a aplikujeme ich na dataset CIFAR-10 resp. CIFAR-100 dotrénovaním pomocou techniky nazývanej prenos učenia (ang. transfer learning). Ide konkrétne o konvolučné siete ResNet 50x1 a ResNet 101x3 [26] dostupné v repozitári [27], MLP Mixer-B/16 [28] a obrazové transformery ViT-B_16 a R50+ViT-B_16 [29] dostupné v repozitári [30].

Pri vyhodnotení na datasete ImageNet1k [31] používame obrazové transformery ViT-Ti_16, ViT-S_16, ViT-B_16, ViT-B_32 [29], MLP mixer Mixer-B/16 [28] a kombináciu konvolučnej siete a obrazového transformera R26+S/32 [32]. Všetky tieto siete sú dostupné v repozitári [30]. Tieto neurónové siete boli predtrénované na kompletnom datasete ImageNet21k [25] a nami prispôsobené na použitie na datasete ImageNet1k dotrénovaním poslednej vrstvy.

## 4.3 Vyhodnotenie na datasete CIFAR-100

Pre lepšie odlíšenie porovnávaných ansámblových metód vytvárame v tomto experimente náročnejšiu úlohu, ako je klasický CIFAR-100. Jej náročnosť spočíva v menšom počte trénovacích dát pre členy ansámblu. Trénovanie členov ansámblu realizujeme na polovici trénovacej množiny datasetu CIFAR-100. Kombinačné metódy a baseline ansámbel trénujeme na náhodne vybranej množine veľkosti 5000 vzoriek z nevyužitej polovice trénovacej množiny.

Náhodné rozdelenie trénovacej množiny a trénovanie neurónových sietí opakujeme 10-krát.

Pri ansámblovaní kombinujeme len siete trénované na rovnakej množine. Získame tak ansámble veľkosti 2 až 4, pričom každý sa opakuje 10-krát pre jednotlivé replikácie trénovania neurónových sietí.

Pre vyhodnotenie sme vybrali dve WLE konfigurácie **logreg_no_interc + m1** a **grad_m2 + m2**. Aby sme lepšie porozumeli správaniu sa testovaných ansámblových

metód, zobrazujeme zlepšenia v sledovaných metrikách oproti najlepšiemu členu ansámblu osobitne pre jednotlivé veľkosti ansámblu. Takéto zobrazenie je na obrázku 3.

Pre baseline ansámbel je vo všetkých troch metrikách s rastúcou veľkosťou ansámblu viditeľný pokles zlepšenia. Podobný pokles je v menšej miere viditeľný aj pre WLE konfiguráciu **grad_m2 + m2**. Pre WLE konfiguráciu **logreg_no_interc + m1** môžeme pozorovať opačný trend, s rastúcou veľkosťou ansámblu zlepšenie v metrike presnosť a NLL rastie, pre metriku ECE nie je trend jednoznačný.

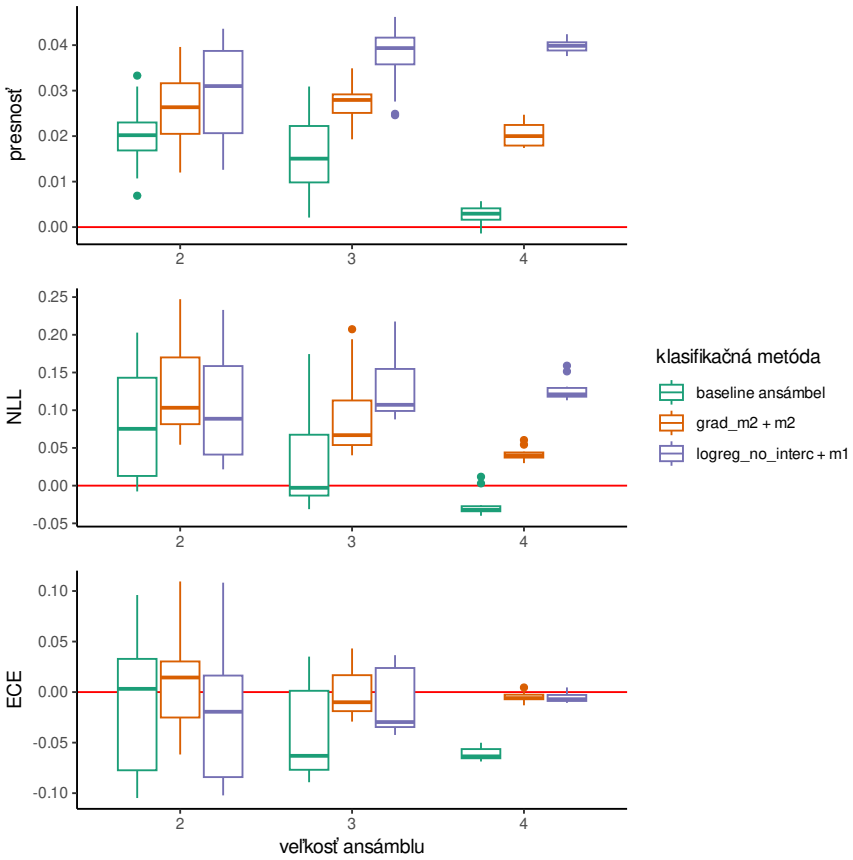
Porovnanie medzi WLE metódami a baseline metódou sme vykonali aj s pomocou štatistických testov. Pre rôzne veľkosti ansámblu sme pozorovali rôzne správanie jednotlivých metód, porovnanie preto vykonávame pre jednotlivé veľkosti ansámblu osobitne. Množiny členov jednotlivých ansámblov nie sú volené pomocou náhodného výberu, používame preto párový permutačný test [33].

Výsledky sme vyhodnotili na hladine významnosti 5%. Vykonané štatistické testy ukázali, že konfigurácie WLE ansámblu s kombinačnou metódou **grad_m2** dosahujú vo všetkých metrikách lepšie výsledky ako baseline ansámbel. Pri WLE konfigurácii s kombinačnou metódou **logreg_no_interc** dochádza k prevahe baseline metódy v prípade metriky ECE a veľkosti ansámblu 2, v ostatných prípadoch vyhráva WLE. Konfigurácie využívajúce kombinačné metódy založené na logistickej regresii dosahujú väčšie zlepšenie v presnosti ako konfigurácie využívajúce gradientové kombinačné metódy.

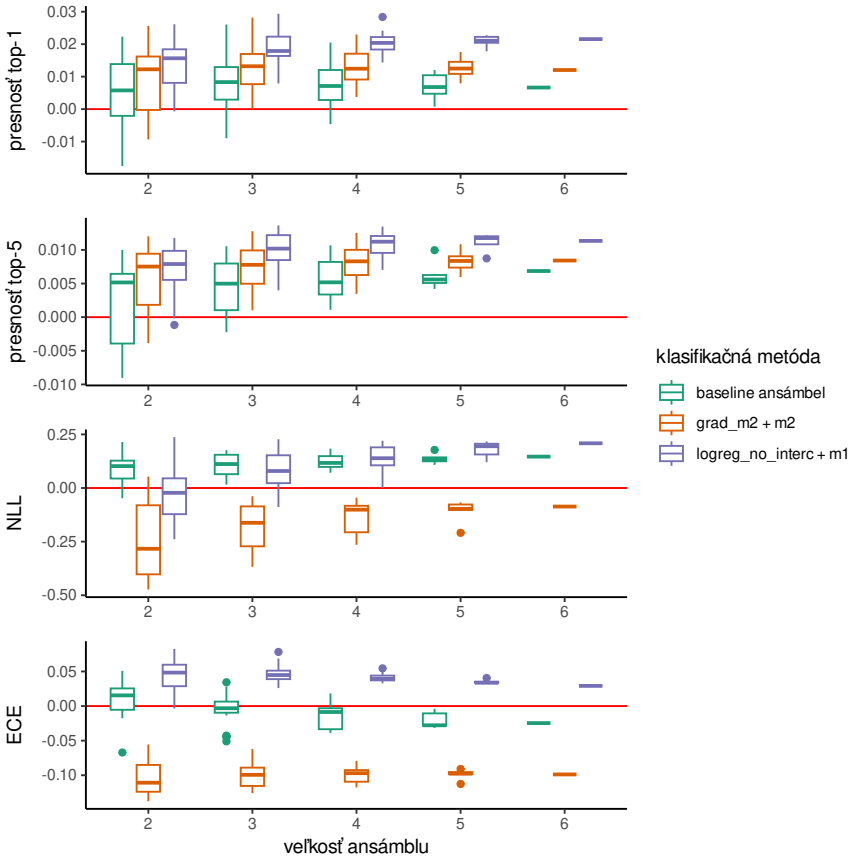
## 4.4 Vyhodnotenie na datasete ImageNet

Pre dataset ImageNet zobrazujeme vyhodnotenie tých istých konfigurácií ako v predchádzajúcej podsekcii. Využívame tu stratégiu zjednodušenej predikcie s odladeným hyperparametrom *topl*. Túto stratégiu predikcie označujeme ako *fast*. Vykonávali sme tiež experimenty bez zjednodušenej predikcie, označované ako *full*, tieto tu ale nie sú zobrazené. Porovnanie s baseline ansámblom pre predikčný prístup *fast* je zobrazené na grafe 4. Baseline ansámbel dosahuje vo všetkých metrikách pre rôzne veľkosti ansámblu prevažne stabilné výsledky. Pre metriku presnosť top-1 a v menšej miere aj pre presnosť top-5 môžeme pozorovať s rastúcou veľkosťou ansámblu zväčšujúcu sa prevahu WLE konfigurácií nad baseline ansámblom. Konfigurácia **logreg_no_interc + m1** dosahuje stabilné zlepšenie oproti najlepšej sieti pre väčšinu prípadov okrem metriky NLL pre veľkosť ansámblu 2. Konfigurácia **grad_m2 + m2** nedosahuje v metrikách NLL a ECE zlepšenie oproti najlepšej sieti.

Z týchto pozorovaní vidíme, že jednotlivé WLE konfigurácie sa správajú pre rôzne veľkosti ansámblu odlišne. Štatistické porovnanie s baseline ansámblom sme preto vykonali pre jednotlivé veľkosti ansámblu osobitne. Pre veľkosti ansámblu 5 a 6 nemáme dostatok vzoriek na vykonanie štatistických testov. Tieto prípady sme




**Obr. 3:** Zlepšenie v sledovaných metrikách oproti najlepšiemu členu ansámblu pre dve konfigurácie WLE z neurónových sietí trénovaných na polovici datasetu CIFAR-100. Veľkosť ansámblu vyjadruje počet jeho členov.




**Obr. 4:** Zlepšenie v sledovaných metrikách oproti najlepšej z kombinovaných sietí pre dve vybrané WLE konfigurácie v závislosti od veľkosti ansámblu na datasete ImageNet1k s prístupom predikcie *fast*.

vyhodnotili vizuálne vykreslením zlepšenia v jednotlivých metrikách, ktoré dosiahli WLE konfigurácie oproti baseline ansámblu. Ide o hodnoty, ktoré sú štandardne spracované v párových štatistických testoch.

Pre ostatné veľkosti ansámblu sme aj tu, podobne ako na datasete CIFAR-100, použili párový permutačný test [33]. Výsledky sme vyhodnotili na hladine významnosti 5%.

Pri predikčnom prístupe *fast* WLE konfigurácia **grad_m2 + m2** prekonáva baseline ansámbel len v metrikách presnosti. Pre metriky NLL a ECE nedosahuje lepšie výsledky ako baseline pre žiadnu veľkosť ansámblu. V prípade použitia klasickej predikcie vyhráva WLE konfigurácia **grad_m2 + m2** nad baseline ansámblom vo všetkých metrikách a pre všetky veľkosti ansámblu. WLE konfigurácia **logreg_no_interc + m1** dosahuje pri predikčnom prístupe *fast* lepšie výsledky. Táto konfigurácia vyhráva nad baseline ansámblom vo všetkých metrikách okrem NLL pri veľkostiach ansámblu 2 a 3, kde výsledky vychádzajú v prospech baseline ansámblu a nerozhodne.

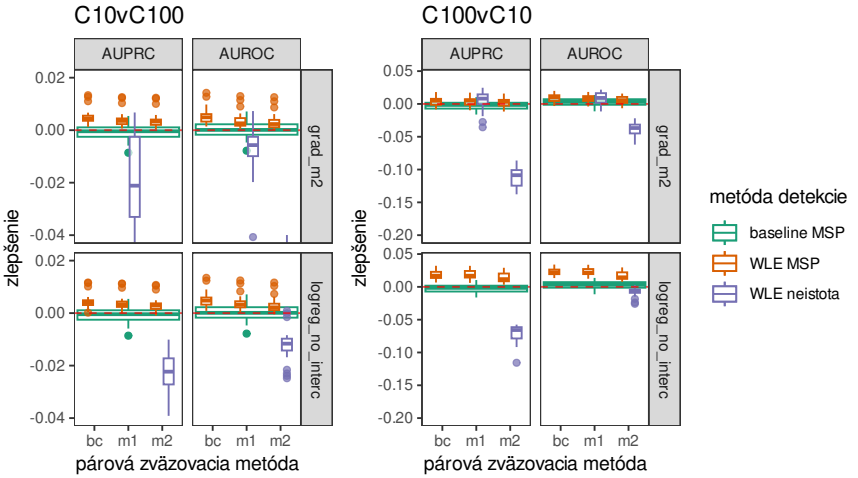
Konfigurácia **grad_m2 + m2** má lepšie správanie pri predikčnom prístupe *full* a prekonáva baseline ansámbel vo všetkých sledovaných metrikách pre všetky veľkosti ansámblov. Konfigurácia **logreg_no_interc + m1** má lepšie správanie pri predikčnom prístupe *fast*. V prípade ansámblov veľkosti 2 a 3 neprekonala baseline ansámbel v metrike NLL, v ostatných prípadoch dosiahla lepšie výsledky ako baseline ansámbel. Vo všeobecnosti odporúčame konfiguráciu **logreg_no_interc + m1** s predikčným prístupom *fast* pre rýchlejší čas jej trénovania aj predikcie a taktiež pre väčšie zlepšenie presnosti oproti konfigurácii **grad_m2 + m2**.

## 4.5 Detekcia neznámych vzoriek

Párové zväzovacie metódy umožňujú kvantifikovať mieru nekonzistencie spracovávaných párových pravdepodobností. V tejto podsekcii skúmame možnosť použitia takto vyjadrenej miery nekonzistencie ako kvantifikátora neistoty pre účel detekcie neznámych vzoriek (ang. out of distribution detection). Ako baseline sme si zvolili zaužívanú metódu najvyššej predikovanej pravdepodobnosti (ang. maximum softmax probability (MSP)), ktorá sa napriek svojej jednoduchosti ukázala ako vysoko úspešná pre viacero aplikácií [18].

Experimenty vykonávame na benchmarkoch CIFAR-10 vs CIFAR-100 a CIFAR-100 vs CIFAR-10. Pri oboch benchmarkoch sú testované klasifikátory natrénované na prvom datasete a testuje sa rozlíšenie testovacej množiny prvého datasetu od testovacej množiny druhého. Testovacia množina druhého datasetu je teda považovaná za "mimo trénovacieho rozdelenia"(ang. out of distribution (OOD)) a testovacia množina prvého datasetu za "v trénovacom rozdelení"(ang. in distribution (IND)).

S baseline metódou detekcie OOD **MSP** sme metódy založené na neistote po-




**Obr. 5:** Zlepšenie metrík AUROC a AUPRC pre jednotlivé testované metódy detekcie neznámych vzoriek oproti najlepšej z kombinovaných sietí. Metódy, ktoré na grafe nie je vidieť dosahovali horšie výsledky. Na ľavom grafe sú zobrazené výsledky pre benchmark CIFAR-10 vs CIFAR-100 a na pravom grafe pre CIFAR-100 vs CIFAR-10. Červenou čiarkovanou čiarou je znázornené nulové zlepšenie.

rovnávali pomocou plôch pod krivkami ROC a PR. Metódu **MSP** sme aplikovali na výstup našej ansámblovej metódy, na výstupy jednotlivých sietí a tiež na výstup baseline ansámblu.

Podobne ako pri ostatných metrikách, aj tu porovnávame zlepšenie dosiahnuté testovanými metódami oproti výsledkom dosiahnutým najlepšou z kombinovaných sietí (s použitím metódy **MSP**). Plochy pod krivkami v nasledujúcich grafoch sú zobrazené v podobe zlepšenia oproti ploche pod zodpovedajúcou krivkou pre tú z kombinovaných sietí, ktorá si v danej metrike počínala najlepšie. Spoločne zobrazujeme výsledky pre detekciu pomocou neistoty z párových zväzovacích metód WLE ako aj pre aplikáciu **MSP** na baseline ansámbel a na výstupy WLE ansámblu. Toto porovnanie je pre obe riešené úlohy zobrazené na obrázku 5. Baseline ansámbel dosahuje podobné výsledky ako najlepšia z kombinovaných sietí. Metódy využívajúce neistotu z párových zväzovacích metód dosahujú stabilné zlepšenie len v konfigurácii **grad_m2 + m1** a len pri úlohe CIFAR-100 vs CIFAR-10. Aplikácia **MSP** na výstupy WLE ansámblu dosahuje zlepšenie vo všetkých konfiguráciách, pre kombinačnú metódu **logreg_no_interc** o niečo výraznejšie ako pre kombinačnú metódu **grad_m2**.

Z praktického dôvodu malého počtu vzoriek pre ansámble veľkosti 4 a 5 a tiež z dôvodu, že sme nenašli špecifické vzory správania sa jednotlivých metód pre rôzne veľkosti ansámblu sme vykonali štatistické porovnanie testovaných metód spoločne pre všetky veľkosti ansámblov. Porovnanie vykonávame medzi metódami využívajúcimi WLE ansámbel a baseline ansámblom s použitím **MSP**. Rovnako ako pri vyhodnocovaní klasifikačných experimentov aj tu používame párový permutačný test [33].

Výsledky boli vyhodnotené na hladine významnosti 5%. Detekcia OOD pomocou neistoty z párových zväzovacích metód priniesla zlepšenie oproti baseline metóde len v konfigurácii **grad_m2 + m1**, a to len na úlohe CIFAR-100 vs CIFAR-10. Metóda, pri ktorej sme aplikovali **MSP** na výstup WLE prekonala baseline v oboch metrikách a na oboch úlohách.

# 5 Záver

V práci sme sa venovali klasifikácii obrazu pomocou strojového učenia. V prvej časti autoreferátu skúmame aktuálny stav ansámblových postupov v klasifikácii a získavame poznatky, ktoré potom využívame pri vytváraní novej ansámblovej klasifikačnej metódy. Zvláštnu pozornosť venujeme párovým ansámblovým modelom, ktoré využívame aj v nami navrhnutej ansámblovej metóde Vážený lineárny ansámbel (WLE).

## Hlavný cieľ práce

V sekcii 3 navrhujeme novú ansámblovú klasifikačnú metódu, ktorá využíva binarizáciu, lineárne klasifikačné metódy a metódy využívané v párových ansámbloch. Navrhujeme viacero verzií tejto metódy, niektoré z nich vyžadujú trénovanie. V sekcii 4 popisujeme experimenty a výsledky prostredníctvom ktorých sme vytvorili metodológiu trénovania a použitia jednotlivých verzií vrátane odladenia ich hyperparametrov. Tiež tu vyhodnocujeme jednotlivé verzie navrhnutej metódy na dvoch datasetoch s počtom tried 100 a 1000. Prostredníctvom týchto experimentov sme splnili hlavný cieľ práce, ktorý sa skladá z nasledujúcich bodov.

- **Efektívne implementovať navrhnutú parametrickú párovú kombinačnú metódu.** Metódu WLE sme implementovali kompletne pomocou tenzorových operácií, vrátane procesu trénovania kombinačných koeficientov. Takáto implementácia umožňuje použiť WLE aj na dataset s 1000 triedami aj napriek kvadratickej zložitosti vzhľadom k počtu tried pri trénovaní. Navrhli sme tiež rozšírenie, ktoré umožňuje zrýchliť proces predikcie pri datasete s 1000 trie-

dami až o dva rády s minimálnym dopadom na kvalitu získanej predikcie. Toto rozšírenie je popísané v sekcii 3.3.

- **Zvoliť vhodnú metódu na vytváranie diverzity použiteľnú pre konvolučné neurónové siete.** V experimentoch sa nám osvedčilo kombinovať rôzne architektúry neurónových sietí. V priebehu posledných rokov si získal veľkú pozornosť výskum v oblasti neurónových sietí nazývaných transformery. Architektúra transformerov bola vo forme obrazových transformerov prispôsobená na prácu s obrazovými dátami a teda aj na klasifikáciu obrazu. Okrem rôznych konvolučných neurónových sietí využívame preto aj niekoľko obrazových transformerov.

- **Zostaviť a otestovať metodiku trénovania kombinačnej metódy.** Vo finálnej podobe metódy WLE sme navrhli niekoľko alternatívnych konfigurácií, všetky z nich vyžadujú trénovanie. Experimentálne sme vybudovali metodiku ich trénovania. Ako najvhodnejšie sa ukázalo používať trénovaciu množinu veľkosti 50 vzoriek na triedu riešenej klasifikačnej úlohy, pozostávajúcu zo vzoriek, ktoré neboli použité pri trénovaní členov ansámblu.

- **Otestovať správanie zostavenej ansámblovej metódy na vhodne zvolených datasetoch.** Metódu WLE sme otestovali na dvoch datasetoch rôznej veľkosti a porovnali sme ju s populárnym priemerovacím ansámblom. Porovnanie na datasete CIFAR-100 je popísané v podsekcii 4.3. Porovnanie na datasete ImageNet1k je popísané v podsekcii 4.4. V tomto prípade sme testovali aj úpravu predikčného procesu WLE umožňujúcu rýchlejšiu predikciu. Konfigurácie WLE prekonali baseline ansámbel vo väčšine testovaných prípadov. Najlepšie výsledky dosahovali konfigurácie **grad_m2 + m2** a **logreg_no_interc + m1**.

## Vedľajší cieľ práce

Párové zväzovacie metódy umožňujú kvantifikovať nesúlad medzi kombinovanými predikciami, čo dáva možnosť využiť ich na detekciu neznámych vzoriek a vytvorenie klasifikátora schopného zdržať sa predikcie. V sekcii 4.5 sme pre našu ansámblovú metódu otestovali aj takéto rozšírenie a porovnali sme ho so štandardne využívanou metódou detekcie neznámych vzoriek MSP. Tieto experimenty napĺňajú vedľajší cieľ práce zložený z nasledovných bodov.

- **Navrhnúť a implementovať funkcionalitu umožňujúcu vytvorenému klasifikátoru zdržať sa klasifikácie.** Teoretický popis tohto rozšírenia je dostupný v sekcii 3.2. Implementovali sme ho pre párové zväzovacie metódy **m1**, **m2** a **bc**.

- **Otestovať implementovanú funkcionalitu na vhodne zvolených úlohách.** Funkcionalitu zdržania sa klasifikácie, resp. detekcie neznámych vzoriek sme otestovali na dvoch úlohách využívajúcich datasety CIFAR-10 a CIFAR-100. Popis experimentov a výsledkov je dostupný v podsekcii 4.5. Implementovanú funkcionalitu sme prostredníctvom metrík AUROC a AUPRC porovnávali s populárnou metódou MSP. Ukázalo sa, že neistota z párových zväzovacích metód neposkytuje dostatočne vhodné informácie na vykonávanie OOD detekcie. Pri experimentoch sme ale zistili, že aplikovanie metódy MSP na výstupy WLE poskytuje lepšiu OOD detekciu, ako aplikovanie MSP na výstupy baseline ansámblu.

## Diskusia

Za hlavnú limitáciu pri použití WLE metódy považujeme potrebu oddelenej trénovacej množiny pre trénovanie kombinačných metód. Pri trénovaní metód hlbokého strojového učenia je spravidla potrebné odladiť hodnoty niekoľkých hyperparametrov na oddelenej validačnej množine. Po odladení hyperparametrov je možné pre dosiahnutie čo najlepších výsledkov znovu natrénovať metódu hlbokého učenia s použitím získaných hodnôt hyperparametrov na kompletnej trénovacej množine zahŕňajúcej aj validačnú množinu. Otestovanie podobného postupu pre použitie WLE metódy je jedným z možných smerovaní ďalšieho výskumu.

Pri teoretickej analýze metódy WLE sme zistili dobré teoretické vlastnosti, ktoré by sa mohli prejaviť pri kombinovaní klasifikátorov poskytujúcich komplementárne informácie. Analýza bola vykonaná po dokončení experimentov v práci, preto návrh vykonaných experimentov tieto vlastnosti nevyužíva. Vhodným spôsobom na otestovanie týchto vlastností by mohla byť klasifikácia multimodálnych dát, pri ktorej sa využíva kombinovanie klasifikátorov trénovaných na odlišných skupinách príznakov [34]. Klasifikácia multimodálnych dát je preto ďalším možným smerovaním budúceho výskumu.

Architektúra WLE metódy technicky umožňuje kombinovanie klasifikátorov zameraných na odlišné podmnožiny tried riešeného problému. Bolo by teda možné identifikovať problematické podmnožiny tried a natrénovať klasifikátory, ktoré by sa na ne špecializovali. S použitím WLE by takéto klasifikátory mohli byť kombinované so štandardnými klasifikátormi zameranými na celý problém. Takéto použitie metódy WLE je taktiež možným smerovaním ďalšieho výskumu.

# Literatúra

[1] A. Rahman, D. V. Smith, and G. Timms, "A novel machine learning approach toward quality assessment of sensor data," *IEEE Sensors Journal*, vol. 14, no. 4, pp. 1035–1047, 2014.

[2] H. Erdoğan, A. Erçil, H. K. Ekenel, S. Y. Bilgin, İ. Eden, M. Kirişçi, and H. Abut, "Multi-modal person recognition for vehicular applications," in *Multiple Classifier Systems* (N. C. Oza, R. Polikar, J. Kittler, and F. Roli, eds.), (Berlin, Heidelberg), pp. 366–375, Springer Berlin Heidelberg, 2005.

[3] V. Svetnik, A. Liaw, C. Tong, and T. Wang, "Application of breiman's random forest to modeling structure-activity relationships of pharmaceutical molecules," in *International Workshop on Multiple Classifier Systems*, pp. 334–343, Springer, 2004.

[4] E. Pranckeviciene, R. Baumgartner, and R. Somorjai, "Using domain knowledge in the random subspace method: Application to the classification of biomedical spectra," in *International Workshop on Multiple Classifier Systems*, pp. 336–345, Springer, 2005.

[5] M. Hosni, I. Abnane, A. Idri, J. M. C. de Gea, and J. L. F. Alemán, "Reviewing ensemble classification methods in breast cancer," *Computer methods and programs in biomedicine*, vol. 177, pp. 89–112, 2019.

[6] L. Hansen and P. Salamon, "Neural network ensembles," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 12, pp. 993 – 1001, 11 1990.

[7] G. Brown, J. Wyatt, R. Harris, and X. Yao, "Diversity creation methods: A survey and categorisation," *Information Fusion*, vol. 6, pp. 5–20, 03 2005.

[8] T. G. Dietterich, "Ensemble methods in machine learning," in *Multiple Classifier Systems*, MCS '00, (Berlin, Heidelberg), p. 1–15, Springer-Verlag, 2000.

[9] L. Rokach, "Ensemble-based classifiers," *Artificial Intelligence Review*, vol. 33, pp. 1–39, 2009.

[10] L. I. Kuncheva, *Combining pattern classifiers: methods and algorithms*. John Wiley & Sons, 2014.

[11] A. K. Seewald and J. Fürnkranz, "An evaluation of grading classifiers," in *International symposium on intelligent data analysis*, pp. 115–124, Springer, 2001.

[12] R. A. Jacobs, M. I. Jordan, S. J. Nowlan, and G. E. Hinton, "Adaptive mixtures of local experts," *Neural computation*, vol. 3, no. 1, pp. 79–87, 1991.

[13] R. Schapire, "The strength of weak learnability," in *30th Annual Symposium on Foundations of Computer Science*, pp. 28–33, 1989.

[14] L. Breiman, "Bagging predictors," *Machine Learning*, vol. 24, pp. 123–140, 08 1996.

[15] T.-F. Wu, C.-J. Lin, and R. C. Weng, "Probability estimates for multi-class classification by pairwise coupling," *Journal of Machine Learning Research*, vol. 5, no. Aug, pp. 975–1005, 2004.

[16] O. Such, S. Benus, and A. Tinajová, "A new method to combine probability estimates from pairwise binary classifiers," in *Conference on Theory and Practice of Information Technologies*, pp. 194–199, 2015.

[17] O. Šuch and S. Barreda, "Bayes covariant multi-class classification," *Pattern Recognition Letters*, vol. 84, pp. 99–106, 2016.

[18] D. Hendrycks and K. Gimpel, "A baseline for detecting misclassified and out-of-distribution examples in neural networks," in *International Conference on Learning Representations*, 2017.

[19] R. Roelofs, N. Cain, J. Shlens, and M. C. Mozer, "Mitigating bias in calibration error estimation," *arXiv preprint arXiv:2012.08668*, 2020.

[20] J. Davis and M. Goadrich, "The relationship between precision-recall and roc curves," in *Proceedings of the 23rd International Conference on Machine Learning*, ICML '06, (New York, NY, USA), p. 233–240, Association for Computing Machinery, 2006.

[21] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (Los Alamitos, CA, USA), pp. 770–778, IEEE Computer Society, 06 2016.

[22] G. Huang, Z. Liu, L. V. D. Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (Los Alamitos, CA, USA), pp. 2261–2269, IEEE Computer Society, 07 2017.

[23] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, (Los Alamitos, CA, USA), pp. 1800–1807, IEEE Computer Society, 07 2017.

[24] A. Radford, J. W. Kim, C. Hallacy, A. Ramesh, G. Goh, S. Agarwal, G. Sastry, A. Askell, P. Mishkin, J. Clark, G. Krueger, and I. Sutskever, "Learning transferable visual models from natural language supervision," in *Proceedings of the 38th International Conference on Machine Learning* (M. Meila and T. Zhang, eds.), vol. 139 of *Proceedings of Machine Learning Research*, pp. 8748–8763, PMLR, 07 2021.

[25] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, "Imagenet: A large-scale hierarchical image database," in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 248–255, 2009.

[26] A. Kolesnikov, L. Beyer, X. Zhai, J. Puigcerver, J. Yung, S. Gelly, and N. Houlsby, "Big transfer (bit): General visual representation learning," in *Computer Vision – ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part V*, (Berlin, Heidelberg), p. 491–507, Springer-Verlag, 2020.

[27] A. Kolesnikov, L. Beyer, X. Zhai, J. Puigcerver, J. Yung, S. Gelly, and N. Houlsby, "Big transfer," 2022.

[28] I. Tolstikhin, N. Houlsby, A. Kolesnikov, L. Beyer, X. Zhai, T. Unterthiner, J. Yung, A. P. Steiner, D. Keysers, J. Uszkoreit, M. Lucic, and A. Dosovitskiy, "MLP-mixer: An all-MLP architecture for vision," in *Advances in Neural Information Processing Systems* (A. Beygelzimer, Y. Dauphin, P. Liang, and J. W. Vaughan, eds.), 2021.

[29] A. Dosovitskiy, L. Beyer, A. Kolesnikov, D. Weissenborn, X. Zhai, T. Unterthiner, M. Dehghani, M. Minderer, G. Heigold, S. Gelly, J. Uszkoreit, and N. Houlsby, "An image is worth 16x16 words: Transformers for image recognition at scale," in *International Conference on Learning Representations*, 2021.

[30] A. Dosovitskiy, L. Beyer, A. Kolesnikov, D. Weissenborn, X. Zhai, T. Unterthiner, M. Dehghani, M. Minderer, G. Heigold, S. Gelly, J. Uszkoreit, and N. Houlsby, "Vision transformer and mlp-mixer architectures," 2022.

[31] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, A. C. Berg, and L. Fei-Fei, "Imagenet large scale visual recognition challenge," *International Journal of Computer Vision*, vol. 115, pp. 211–252, 2015.

[32] A. P. Steiner, A. Kolesnikov, X. Zhai, R. Wightman, J. Uszkoreit, and L. Beyer, "How to train your vit? data, augmentation, and regularization in vision transformers," *Transactions on Machine Learning Research*, 2022.

[33] S. S. Mangiafico, *Summary and Analysis of Extension Program Evaluation in R*. New Brunswick, NJ: Rutgers Cooperative Extension, 1.20.01 ed., 2016.

[34] E. Alpaydin, *Classifying Multimodal Data*, p. 49–69. Association for Computing Machinery and Morgan & Claypool, 2018.

# 6 Zoznam publikácií autora

**ADF Innovating instruction of communication theory with machine learning and speech analysis** - ICETA 2020: 18th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning : proceedings / Jakab, František [editor]. – 1. vyd. – Denver (USA) : Institute of Electrical and Electronics Engineers, 2020. – ISBN 978-0-7381-2366-0, s. [680-686].

Šuch Ondrej (45%), Fabricius René (45%), Klimo Martin (5%), Juhár Jozef (5%)

**AFD Ensemble classification methods** - Mathematics in science and technologies: proceedings of the MIST conference 2021 / Bachratá, Katarína; Bohiniková, Alžbeta. – 1. vyd. – [S.l.] : [s.n.], 2021. – ISBN 9798748088183, s. [26-36].

Fabricius René (100%)

**ADF Detection of vowel segments in noise with ImageNet neural network architectures** - TRANSCOM 2021: 14th International Scientific Conference on Sustainable, Modern and Safe Transport : (2021) Transportation Research Procedia, 55. - ISSN 23521457, s. [1289-1295].

Fabricius René (50%), Šuch Ondrej (50%)

**ADN Two objective public service system design problem** - Communications: scientific letters of the University of Žilina. - ISSN 1335-4205. - Roč. 23, č. 4 (2021), s. [68-75].

Janáček Jaroslav (25%), Koháni Michal (25%), Grygar Dobroslav (25%), Fabricius René (25%)

**ADC Public service system design with conflicting criteria** - IEEE Access: practical innovations, open solutions. - ISSN 2169-3536. - Roč. 9 (2021), s. 130665-130679.

Janáček Jaroslav (50%), Fabricius René (50%)

**ADF Introducing students to out-of-distribution detection with deep neural networks** - ICETA 2022: 20th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning : proceedings. 2020. – ISBN 979-8-3503-2033-6, s. [627-633].

Šuch Ondrej (50%), Fabricius René (45%), Tarábek Peter (5%)

**Bridging performance gap between minimal and maximal SVM models** - Transactions on Machine Learning Research - ISSN 2835-8856. (2023) https://openreview.net/forum?id=SM1BkjGePI

Šuch Ondrej, Fabricius René